IMPLEMENTIERUNGSLEITFADEN

# EMC VSPEX-ANWENDER-COMPUTING

## VMware Horizon 6.0 mit View und VMware vSphere für bis zu 2.000 virtuelle Desktops

### Unterstützt durch EMC VNX und EMC Data Protection

## EMC VSPEX

### Überblick

In diesem Implementierungsleitfaden werden die allgemeinen Schritte für die Bereitstellung einer EMC® VSPEX®-Lösung für Anwender-Computing für VMware Horizon View und VMware vSphere mit EMC VNX® und EMC Data Protection beschrieben.

Oktober 2014

EMC²

Copyright © 2014 EMC Deutschland GmbH. Alle Rechte vorbehalten. Veröffentlicht in Deutschland.

Veröffentlicht im Oktober 2014

EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Die Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Die Informationen in dieser Veröffentlichung werden ohne Gewähr zur Verfügung gestellt. Die EMC Corporation macht keine Zusicherungen und übernimmt keine Haftung jedweder Art im Hinblick auf die in diesem Dokument enthaltenen Informationen und schließt insbesondere jedwede implizite Haftung für die Handelsüblichkeit und die Eignung für einen bestimmten Zweck aus. Für die Nutzung, das Kopieren und die Verbreitung der in dieser Veröffentlichung beschriebenen EMC Software ist eine entsprechende Softwarelizenz erforderlich.

EMC², EMC und das EMC Logo sind eingetragene Marken oder Marken der EMC Corporation in den USA und anderen Ländern. Alle anderen in diesem Dokument erwähnten Marken sind das Eigentum ihrer jeweiligen Inhaber.

Eine aktuelle Liste der Produkte von EMC finden Sie unter EMC Corporation Trademarks auf http://germany.emc.com.

**EMC VSPEX-Anwender-Computing**
**VMware Horizon 6.0 mit View und VMware vSphere für bis zu 2.000 virtuelle Desktops**
**Unterstützt durch EMC VNX und EMC Data Protection**
**Implementierungsleitfaden**

Art.-Nr. H13573

# Inhalt

**Kapitel 1 Einführung 9**
Zweck dieses Leitfadens ..... 10
Geschäftlicher Nutzen ..... 10
Umfang ..... 11
Zielgruppe ..... 11
Terminologie ..... 12

**Kapitel 2 Bevor Sie beginnen 13**
Übersicht ..... 14
Aufgaben vor der Bereitstellung ..... 14
Bereitstellungsworkflow ..... 15
Grundlegende Dokumente ..... 16
Voraussetzungen für die Bereitstellung ..... 16

**Kapitel 3 Lösungsüberblick 19**
Übersicht ..... 20
VSPEX Proven Infrastructures ..... 20
Lösungsarchitektur ..... 21
Allgemeine Architektur ..... 21
Logische Architektur ..... 23
Übersicht über die Kernkomponenten ..... 24

**Kapitel 4 Lösungsimplementierung 25**
Übersicht ..... 26
Netzwerkimplementierung ..... 27
Konfigurieren des Infrastrukturnetzwerks ..... 27
Konfigurieren der virtuellen LANs ..... 28
Konfigurieren des Speichernetzwerks (Blockvariante) ..... 29
Vervollständigen der Netzwerkverkabelung ..... 29
Vorbereiten und Konfigurieren des Speicherarrays ..... 30
Vorbereiten der VNX ..... 31
Einrichten der anfänglichen VNX-Konfiguration ..... 31
Provisioning von Kerndatenspeicher ..... 31
Provisioning von Speicher für VMFS-Datastores (nur Block) ..... 31
Provisioning von Speicher für NFS-Datastores (nur File) ..... 32
Konfigurieren von FAST Cache ..... 35
Provisioning von optionalem Speicher für Benutzerdaten ..... 37
Konfigurieren von FAST VP für Benutzerdaten ..... 38

Provisioning von optionalem Speicher für virtuelle Infrastrukturmaschinen ... 40
Festlegen von Schwellenwerten und Warnmeldungen für Virtual Provisioning ... 40
Installieren und Konfigurieren der vSphere-Hosts ... 42
Installieren von vSphere ... 43
Konfigurieren des vSphere-Netzwerks ... 43
Verbinden der VMware-Datastores ... 44
Installieren und Konfigurieren der SQL Server-Datenbank ... 44
Bereitstellen von VMware vCenter Server ... 45
Einrichten von VMware Horizon View Connection Server ... 47
Erstellen virtueller Maschinen für VMware Horizon View Connection Server ... 48
Installieren von VMware Horizon View Connection Server ... 48
Konfigurieren der Verbindung zur View-Eventprotokolldatenbank ... 48
Hinzufügen einer Replikatinstanz von View Connection Server ... 48
Konfigurieren der View Composer-ODBC-Verbindung ... 49
Installieren von View Composer ... 49
Verbinden von VMware Horizon View mit vCenter und View Composer ... 49
Vorbereiten einer virtuellen Mastermaschine ... 49
Konfigurieren von View Persona Management-Gruppen-Policies ... 50
Konfigurieren der Gruppen-Policies für die Ordnerumleitung für EMC Avamar ... 50
Konfigurieren von View PCoIP-Gruppen-Policies ... 50
Provisioning von virtuellen Desktops ... 50
Einrichten von EMC Avamar ... 52
Einrichten von VMware vShield Endpoint ... 52
Überprüfen der Desktoptreiberinstallation für vShield Endpoint ... 53
Bereitstellen der vShield Manager-Appliance ... 53
Installieren des vShield Endpoint-Service ... 53
Bereitstellen eines Managementservers für die Virenschutzlösung ... 53
Bereitstellen der virtuellen vSphere-Sicherheitsmaschinen ... 53
Überprüfen der vShield Endpoint-Funktion ... 53
Einrichten von VMware Horizon Workspace ... 54
Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen ... 57
Gewähren der SMTP-Relayberechtigungen für Workspace ... 57
Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für Workspace ... 57
Konfigurieren einer CIFS-Share zur Verwendung als ThinApp-Repository (optional) ... 57
Überprüfen der angegebenen E-Mail-Adressen aller Workspace-Benutzer ... 58
Bereitstellen einer Workspace-Appliance in vCenter ... 58
Erlangen der Informationen, die zum Aktivieren der Workspace-Integration mit Active Directory erforderlich sind ... 58
Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die Horizon Workspace-Appliance (optional) ... 58

Konfigurieren des externen Zugriffs auf die Workspace-Appliance (optional) ..... 59
Aktivieren der Horizon View-Integration (optional) ..... 59
Einrichten von VMware vCenter Operations Manager for Horizon View ..... 59

**Kapitel 5 Lösungsüberprüfung 61**
Übersicht ..... 62
Checkliste nach der Installation ..... 63
Bereitstellen und Testen eines einzigen virtuellen Desktops ..... 63
Überprüfen der Redundanz der Lösungskomponenten ..... 63

**Kapitel 6 Referenzdokumentation 65**
EMC Dokumentation ..... 66
Andere Dokumentationen ..... 66

**Anhang A Konfigurationsarbeitsblatt 69**
Arbeitsblatt für die Kundenkonfiguration ..... 70

## Abbildungen

Abbildung 1. VSPEX Proven Infrastructures ..... 21
Abbildung 2. Architektur der validierten Lösung ..... 22
Abbildung 3. Logische Architektur für Block- und File-basierten Speicher ..... 23
Abbildung 4. Beispiel-Ethernetnetzwerkarchitektur ..... 28
Abbildung 5. Beispiel für eine Fibre-Channel-Netzwerkarchitektur ..... 29
Abbildung 6. Anzeigen aller Data Mover-Parameter ..... 34
Abbildung 7. Festlegen von nthread-Parametern ..... 35
Abbildung 8. Dialogfeld Storage System Properties ..... 35
Abbildung 9. Dialogfeld Create FAST Cache ..... 36
Abbildung 10. Dialogfeld Storage Pool Properties ..... 38
Abbildung 11. Das Fenster Manage Auto-Tiering ..... 39
Abbildung 12. Das Fenster LUN Properties ..... 39
Abbildung 13. Überprüfen der Speicherplatzauslastung des Speicherpools ..... 40
Abbildung 14. Definieren der Schwellenwerte für die Speicherpoolauslastung ..... 41
Abbildung 15. Definieren automatisierter Benachrichtigungen für Block ..... 41
Abbildung 16. Das Fenster View Composer Disks ..... 51
Abbildung 17. Öffnen von Anhängen in einer PDF-Datei ..... 70

## Tabellen


Tabelle 1. Terminologie ... 12
Tabelle 2. Aufgaben vor der Bereitstellung ... 14
Tabelle 3. Bereitstellungsworkflow ... 15
Tabelle 4. Checkliste für die Bereitstellungsvoraussetzungen ... 16
Tabelle 5. Lösungskomponenten ... 24
Tabelle 6. Übersicht über den Implementierungsprozess ... 26
Tabelle 7. Aufgaben für die Switch- und Netzwerkkonfiguration ... 27
Tabelle 8. Aufgaben für die Speicherkonfiguration ... 30
Tabelle 9. Erstellen eines blockbasierten RAID-5-Speicherpools ... 31
Tabelle 10. LUNs auf der VNX zum Speichern virtueller Desktops ... 32
Tabelle 11. Erstellen eines blockbasierten RAID-5-Speicherpools ... 32
Tabelle 12. Konfigurieren von LUNs für NAS-Pools ... 33
Tabelle 13. Konfigurieren von Dateisystemen als NFS-Datastores ... 34
Tabelle 14. Erstellen eines blockbasierten RAID-6-Speicherpools ... 37
Tabelle 15. Konfigurieren von LUNs für NAS-Pools ... 38
Tabelle 16. VMX-Schwellenwerte und -Einstellungen ... 42
Tabelle 17. Aufgaben für die Serverinstallation ... 42
Tabelle 18. Aufgaben für die SQL Server-Datenbankkonfiguration ... 44
Tabelle 19. Aufgaben für die vCenter-Konfiguration ... 45
Tabelle 20. Aufgaben für die Einrichtung von VMware Horizon View Connection Server ... 47
Tabelle 21. Für die Installation und Konfiguration von vShield Endpoint erforderliche Aufgaben ... 52
Tabelle 22. Aufgaben beim Einrichten von VMware Horizon Workspace ... 54
Tabelle 23. Für die Installation und Konfiguration von vCenter Operations Manager erforderliche Aufgaben ... 59
Tabelle 24. Aufgaben für das Testen der Installation ... 62
Tabelle 25. Allgemeine Serverinformationen ... 71
Tabelle 26. vSphere-Serverinformationen ... 71
Tabelle 27. Arrayinformationen ... 71
Tabelle 28. Informationen zur Netzwerkinfrastruktur ... 72
Tabelle 29. VLAN-Informationen ... 72
Tabelle 30. Servicekonten ... 72

# Kapitel 1 Einführung

In diesem Kapitel werden die folgenden Themen behandelt:

**Zweck dieses Leitfadens** ..... 10

**Geschäftlicher Nutzen** ..... 10

**Umfang** ..... 11

**Zielgruppe** ..... 11

**Terminologie** ..... 12

## Zweck dieses Leitfadens

Mit der EMC® VSPEX®-Anwender-Computing-Architektur erhält der Kunde ein modernes System, mit dem eine große Zahl virtueller Desktops auf einem konsistenten Performancelevel gehostet werden kann. Diese VSPEX-Lösung für Anwender-Computing für VMware Horizon 6.0 mit View wird auf einer VMware vSphere-Virtualisierungsebene ausgeführt, die von der hochverfügbaren EMC VNX®-Produktreihe unterstützt wird, die den Speicher bereitstellt. Sie ist für die Ausführung auf einer VSPEX Private Cloud für VMware vSphere Proven Infrastructure ausgelegt.

Die Rechner- und Netzwerkkomponenten, die von den VSPEX-Partnern definiert werden, sind redundant und ausreichend leistungsstark ausgelegt, um die Verarbeitungs- und Datenanforderungen großer virtueller Maschinenumgebungen zu verarbeiten. EMC Avamar® Data Protection-Lösungen bieten Datensicherheit für VMware Horizon View-Daten und RSA® SecurID® bietet optionale Funktionen für die sichere Benutzerauthentifizierung.

Diese VSPEX-Lösung für Anwender-Computing wird an 3 verschiedenen Skalierungspunkten validiert: bei 500, 1.000 und 2.000 virtuellen Desktops. Die validierten Konfigurationen basieren auf einem Referenzdesktop-Workload und bilden die Basis für wirtschaftliche, benutzerdefinierte Lösungen für einzelne Kunden. Eine kleinere virtuelle Desktopumgebung für die Bereitstellung von bis zu 500 Desktops auf Basis von EMC VNXe® 3200 wird hier beschrieben: *EMC VSPEX-Anwender-Computing: VMware Horizon 6.0 mit View und VMware vSphere 5.5 für bis zu 500 virtuelle Desktops – Designleitfaden*.

Eine Infrastruktur für Anwender-Computing oder virtuelle Desktops ist ein komplexes Systemangebot. In diesem Implementierungsleitfaden wird beschrieben, wie Sie mithilfe von Best Practices die erforderlichen Ressourcen implementieren, um eine Anwender-Computing-Lösung unter Verwendung von VMware Horizon View für VMware vSphere mit Unterstützung durch EMC VNX und EMC Data Protection bereitzustellen.

## Geschäftlicher Nutzen

Mitarbeiter sind mobiler als je zuvor. Sie erwarten jederzeit, überall und von jedem beliebigen Gerät aus Zugriff auf wichtige Geschäftsdaten und Anwendungen. Sie möchten ihre eigenen Geräte zur Arbeit mitbringen können, sodass IT-Abteilungen zunehmend BYOD-Initiativen (Bring Your Own Device) in Erwägung ziehen. Dadurch nimmt die Komplexität in Bezug auf den Schutz von vertraulichen Informationen zu. Die Bereitstellung virtueller Desktops bietet hier eine Möglichkeit. Hinzu kommt die Tatsache, dass Geschäftsanwendungen zunehmend in eine konsolidierte Rechner-, Netzwerk- und Speicherumgebung übertragen werden. Es handelt sich also um einen grundlegenden Paradigmenwechsel.

Diese VSPEX-Lösung für Anwender-Computing mit VMware reduziert die Komplexität, die bei der Konfiguration der einzelnen Komponenten eines herkömmlichen Bereitstellungsmodells auftritt. Das Integrationsmanagement wird vereinfacht. Gleichzeitig bleiben die Design- und Implementierungsoptionen von Anwendungen erhalten. Zudem werden die Administration vereinheitlicht und Kontrolle und Monitoring über die Prozesstrennung ermöglicht.

Die VSPEX-Lösung für Anwender-Computing für VMware Horizon View bietet unter anderem die folgenden geschäftlichen Vorteile:

- Bereitstellen einer End-to-End-Virtualisierungslösung zur Nutzung der Funktionen von einheitlichen Infrastrukturkomponenten
- Effiziente Virtualisierung von bis zu 2.000 virtuellen Desktops für verschiedene Kundenanwendungsbeispiele
- Zuverlässige, flexible und skalierbare Referenzarchitekturen

## Umfang

Dieser Implementierungsleitfaden beschreibt die allgemeinen Schritte für eine Bereitstellung der VSPEX-Lösung für Anwender-Computing für VMware Horizon View 6.0 mit View, die in einer VSPEX Private Cloud für VMware vSphere Proven Infrastructure ausgeführt wird. Der Leitfaden enthält Beispiele für Bereitstellungen in EMC Speicherarrays VNX5200, VNX5400 und VNX5600. Dieselben Prinzipien und Richtlinien gelten auch für alle VNX-Modelle, die im Rahmen des VSPEX-Programms validiert wurden.

Die EMC Data Protection-Lösungen für die Datensicherheit in VMware Horizon View werden in einem separaten Dokument beschrieben: *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View*.

Die optionale Lösung für die sichere Benutzerauthentifizierung RSA SecurID für VMware Horizon View wird ebenfalls in einem separaten Dokument beschrieben, *Sicherung des EMC VSPEX-Anwender-Computing mit RSA SecurID: VMware Horizon View 5.2 und VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden*.

## Zielgruppe

Dieser Leitfaden richtet sich an interne Mitarbeiter von EMC und qualifizierte EMC VSPEX-Partner. In diesem Leitfaden wird davon ausgegangen, dass VSPEX-Partner, die beabsichtigen, diese VSPEX Proven Infrastructure für VMware Horizon View bereitzustellen, über die erforderliche Schulung und den entsprechenden Hintergrund verfügen, um eine Anwender-Computing-Lösung auf der Basis von Horizon View mit VMware vSphere als Hypervisor, das VNX-Speichersystem und die damit verbundene Infrastruktur installieren und konfigurieren zu können.

Leser sollten außerdem mit den Infrastruktur- und Datenbanksicherheitsrichtlinien der Kundeninstallation vertraut sein.

In diesem Leitfaden werden gegebenenfalls externe Referenzen bereitgestellt. Partner, die diese Lösung implementieren, sollten mit diesen Dokumenten vertraut sein. Weitere Details finden Sie unter Grundlegende Dokumente und in Kapitel 6: Referenzdokumentation.

# Terminologie

Tabelle 1 führt die in diesem Handbuch verwendete Terminologie auf.

**Tabelle 1. Terminologie**

| Begriff | Definition |
|---|---|
| EUC | Entkoppelt den Desktop von der physischen Maschine. In einer EUC-Umgebung befinden sich das Desktopbetriebssystem und die Anwendungen auf einer virtuellen Maschine, die auf einem Hostcomputer ausgeführt wird. Die Daten befinden sich im gemeinsamen Speicher. Die Benutzer können von jedem Computer oder Mobilgerät aus über ein privates Netzwerk oder eine Internetverbindung auf ihren virtuellen Desktop zugreifen. |
| Verknüpfte Clones | Als verknüpfte Clones bereitgestellte Desktops verwenden ein gemeinsames Basis-Image innerhalb eines Desktoppools und belegen deshalb nur wenig Platz im Speicher. |
| Referenzarchitektur | Die validierte Architektur, die diese VSPEX-Anwender-Computing-Lösung bei einem bestimmten Umfang unterstützt – in diesem Fall bis zu 500, 1.000 oder 2.000 virtuelle Desktops |
| Speicherprozessor (SP) | Der Speicherprozessor ist die Rechnerkomponente des Speicherarrays. SPs werden für alle Aspekte der Datenverlagerung in, aus und zwischen Arrays eingesetzt. |

# Kapitel 2 Bevor Sie beginnen

In diesem Kapitel werden die folgenden Themen behandelt:

**Übersicht** ..... 14

**Aufgaben vor der Bereitstellung** ..... 14

**Bereitstellungsworkflow** ..... 15

**Grundlegende Dokumente** ..... 16

**Voraussetzungen für die Bereitstellung** ..... 16

# Übersicht

In diesem Kapitel erhalten Sie einen Überblick über wichtige Informationen, die Sie haben müssen, Dokumente, mit denen Sie vertraut sein, und Aufgaben, die Sie ausführen müssen, bevor Sie mit der Implementierung der VSPEX-Lösung für Anwender-Computing mit VMware Horizon View beginnen.

Im Designleitfaden für diese Lösung – *EMC VSPEX-Anwender-Computing: VMware Horizon 6.0 mit View und VMware vSphere für bis zu 2.000 virtuelle Desktops* wird beschrieben, wie Sie Ihre Lösung entwerfen und dimensionieren, Ressourcen gemäß Best Practices zuweisen und alle Vorteile von VSPEX nutzen. Die Beispiele für Bereitstellungen in diesem Implementierungsleitfaden beruhen auf den Empfehlungen und Beispielen des Designleitfadens.

# Aufgaben vor der Bereitstellung

Zu den Aufgaben vor der Bereitstellung zählen Verfahren, die nicht direkt mit der Installation und Konfiguration der Umgebung zusammenhängen, sondern deren Ergebnisse zum Zeitpunkt der Installation benötigt werden. Beispiele für Aufgaben vor der Bereitstellung sind das Sammeln von Hostnamen, IP-Adressen, VLAN-IDs, Lizenzschlüsseln, Installationsmedien und so weiter. Diese Aufgaben sollten vor dem Besuch beim Kunden erledigt werden, um den Zeitaufwand vor Ort so gering wie möglich zu halten.

**Tabelle 2. Aufgaben vor der Bereitstellung**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Sammeln von Dokumenten | Sammeln Sie die in Grundlegende Dokumente und Referenzdokumentation aufgeführten Dokumente. Diese werden im gesamten Dokument dafür verwendet, Details zu Einrichtungsverfahren und Dimensionierung sowie Best Practices für die Bereitstellung der verschiedenen Komponenten der Lösung zur Verfügung zu stellen. | • Grundlegende Dokumente<br>• Referenzdokumentation |
| Sammeln von Tools | Sammeln Sie die erforderlichen und optionalen Tools für die Bereitstellung. Verwenden Sie Tabelle 4, um zu überprüfen, ob die gesamte Hardware, Software und die entsprechenden Lizenzen vor dem Bereitstellungsprozess verfügbar sind. | Checkliste für die Bereitstellungsvoraussetzungen |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Sammeln von Daten | Sammeln Sie die kundenspezifischen Konfigurationsdaten für Netzwerk, Arrays, Konten usw. Geben Sie diese Daten in das Arbeitsblatt für die Kundenkonfiguration ein, das Sie während des Bereitstellungsprozesses als Referenz verwenden können.<br>Füllen Sie zusätzlich das entsprechende VNX-Arbeitsblatt aus, um umfassende arrayspezifische Informationen zur Hand zu haben. Diese Arbeitsblätter stehen auf der EMC Online Support-Website zur Verfügung. | • *Konfigurationsarbeitsblatt für VNX Block*<br>• *VNX Installation Assistant for File/Unified – Arbeitsblatt*<br>• Arbeitsblatt für die Kundenkonfiguration |

## Bereitstellungsworkflow

Ziehen Sie für das Design und die Implementierung Ihrer Anwender-Computing-Lösung den Prozessablauf in Tabelle 3[1] zurate.

**Tabelle 3. Bereitstellungsworkflow**

| Schritt | Aktion |
|---|---|
| 1 | Verwenden Sie das Arbeitsblatt für die Kundenkonfiguration im Designleitfaden, um Kundenanforderungen zu erfassen. |
| 2 | Verwenden Sie das EMC VSPEX-Dimensionierungstool, um die empfohlene VSPEX-Referenzarchitektur für Ihre Anwender-Computing-Lösung auf Basis der in Schritt 1 erfassten Kundenanforderungen zu ermitteln.<br>Weitere Informationen zum Dimensionierungstool finden Sie im Portal zum EMC VSPEX-Dimensionierungstool.<br>**Hinweis:** Sollte das Dimensionierungstool nicht zur Verfügung stehen, können Sie die Anwendung anhand der Richtlinien im Designleitfaden manuell dimensionieren. |
| 3 | Legen Sie das endgültige Design der VSPEX-Lösung mithilfe des Designleitfadens fest.<br>**Hinweis:** Sorgen Sie dafür, dass alle Ressourcenanforderungen und nicht nur die Anforderungen für das Anwender-Computing berücksichtigt werden. |
| 4 | Wählen und bestellen Sie die geeignete VSPEX-Referenzarchitektur und Proven Infrastructure. Empfehlungen zur Auswahl einer Private Cloud Proven Infrastructure finden Sie im VSPEX Proven Infrastructure-Leitfaden unter Grundlegende Dokumente. |

[1] Wenn Ihre Lösung Komponenten zur Datensicherheit umfasst, finden Sie Richtlinien zur Dimensionierung der Datensicherheit sowie Implementierungsanweisungen im *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View*.

| Schritt | Aktion |
|---|---|
| 5 | Befolgen Sie diesen Implementierungsleitfaden zum Bereitstellen und Testen Ihrer VSPEX-Lösung.<br>**Hinweis**: Wenn Sie bereits über eine VSPEX Proven Infrastructure-Umgebung verfügen, können Sie die bereits abgeschlossenen Schritte für die Implementierung überspringen. |

## Grundlegende Dokumente

EMC empfiehlt, die folgenden Dokumente zu lesen, die Sie im Bereich „VSPEX“ im EMC Community Network oder unter http://germany.emc.com oder im VSPEX Proven Infrastructure-Partnerportal finden.

- E*MC VSPEX-Lösungen für Anwender-Computing mit VMware vSphere und VMware View*
- *EMC VSPEX-Anwender-Computing: VMware Horizon View 6.0 und VMware vSphere für bis zu 2.000 virtuelle Desktops*
- *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 1.000 virtuelle Maschinen*
- *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View*

## Voraussetzungen für die Bereitstellung

Tabelle 4 gibt die Hardware-, Software- und Lizenzanforderungen für die Konfiguration der Lösung an. Weitere Informationen zu diesen Anforderungen finden Sie auf der EMC Online Support-Website.

**Tabelle 4. Checkliste für die Bereitstellungsvoraussetzungen**

| Anforderung | Beschreibung |
|---|---|
| Hardware | • Physische Server mit ausreichend Kapazität zum Hosten der virtuellen Desktops gemäß den Empfehlungen im Designleitfaden<br>• VMware vSphere-Server zum Hosten der virtuellen Infrastrukturserver<br>• Für das Anwender-Computing erforderliche Netzwerkswitch-Portkapazität und -funktionen<br>• EMC VNX-Multiprotokoll-Speicherarray mit dem erforderlichen Laufwerkslayout<br>**Hinweis**: Diese Anforderungen werden möglicherweise durch die vorhandene Infrastruktur erfüllt. |

| Anforderung | Beschreibung |
|---|---|
| Software | • Installationsmedien für VMware vSphere 5.5<br>• Installationsmedien für VMware vCenter Server 5.5<br>• VMware vShield Manager OVA-Datei (Open Virtualization Appliance)<br>• VMware vCenter Operations Manager OVA-Datei<br>• VMware vCenter Operations Manager for Horizon View Adapter<br>• VMware Horizon 6.0 mit View – Installationsdateien<br>• Management-Serversoftware für die VMware vShield Endpoint-Virenschutzlösung von Partnern<br>• VMware vShield Endpoint-Partnersoftware für die Sicherheit von virtuellen Maschinen<br>• EMC Virtual Storage Integrator (VSI) für VMware vSphere Web Client OVA-Datei<br>• Installationsmedien für Microsoft Windows Server 2012 R2 (empfohlenes Betriebssystem für VMware vCenter und VMware Horizon View Connection Server)<br>• Installationsmedien für Microsoft Windows 8.1<br>• Installationsmedien für Microsoft SQL Server 2012<br>**Hinweis**: Diese Anforderung wird möglicherweise durch die vorhandene Infrastruktur erfüllt. |
| Software (nur Blockvariante) | • EMC PowerPath® Viewer<br>• EMC PowerPath Virtual Edition (PowerPath/VE) |
| Software (nur File-basierte Variante) | • VAAI-Plug-in (VMware Storage APIs for Array Integration) für VNX for File |
| Lizenzen | • Lizenzschlüssel für VMware vCenter 5.5<br>• Lizenzschlüssel für VMware vSphere Desktop<br>• Lizenzschlüssel für VMware Horizon 6.0 mit View<br>• Lizenzschlüssel für VMware vShield Endpoint (VMware)<br>• Lizenzschlüssel für VMware vShield Endpoint (vShield-Partner)<br>• VMware vCenter Operations Manager for VMware Horizon View<br>• Lizenzschlüssel für Microsoft Windows Server 2012 R2 Standard Edition (oder höher)<br>**Hinweis**: Diese Anforderung wird möglicherweise durch einen vorhandenen Microsoft KMS (Key Management Server) erfüllt.<br>• Lizenzschlüssel für Microsoft Windows 8.1<br>**Hinweis**: Diese Anforderung wird möglicherweise durch einen vorhandenen Microsoft KMS erfüllt.<br>• Lizenzschlüssel für Microsoft SQL Server<br>**Hinweis**: Diese Anforderung wird möglicherweise durch eine vorhandene Lizenz erfüllt. |
| Lizenzen (nur Blockvariante) | • Lizenzdateien für EMC PowerPath Virtual Edition |

# Kapitel 3 Lösungsüberblick

In diesem Kapitel werden die folgenden Themen behandelt:

**Übersicht** ..... **20**

**VSPEX Proven Infrastructures** ..... **20**

**Lösungsarchitektur** ..... **21**

**Übersicht über die Kernkomponenten** ..... **24**

# Übersicht

In diesem Kapitel finden Sie einen Überblick über die VSPEX-Lösung für Anwender-Computing für VMware Horizon View mit VMware vSphere und die wichtigsten in der Lösung verwendeten Technologien. Die Lösung wurde von EMC entwickelt und erprobt und bietet die für den Support von Referenzarchitekturen mit 3 Skalierungspunkten erforderlichen Ressourcen für Desktopvirtualisierung, Server, Netzwerk, Speicher und Datensicherheit: 500, 1.000 und 2.000 virtuelle Desktops.

Obwohl die Lösung für die Ausführung auf einer VSPEX Private Cloud-Lösung ausgelegt ist, umfassen die Referenzarchitekturen keine Konfigurationsdetails für die zugrunde liegende Proven Infrastructure. Informationen zur Konfiguration der erforderlichen Infrastrukturkomponenten finden Sie in den VSPEX Proven Infrastructure-Leitfäden unter Grundlegende Dokumente.

# VSPEX Proven Infrastructures

EMC hat gemeinsam mit den branchenführenden Anbietern von IT-Infrastrukturen eine umfassende Virtualisierungslösung entwickelt, die die Bereitstellung der Private Cloud und der virtuellen VMware Horizon View-Desktops beschleunigt. Mit VSPEX sind Kunden in der Lage, die Transformation ihrer IT durch schnellere Bereitstellung, verbesserte Anwenderfreundlichkeit, größere Auswahl, höhere Effizienz und weniger Risiko zu beschleunigen. Dadurch wird die Erstellung der IT-Infrastruktur vereinfacht.

Die VSPEX-Validierung durch EMC bietet eine zuverlässige Performance und ermöglicht Kunden die Auswahl von Technologien, die ihre vorhandene oder neu erworbene IT-Infrastruktur nutzen und so den Planungs-, Dimensionierungs- und Konfigurationsaufwand vermeiden. VSPEX stellt eine virtuelle Infrastruktur für Kunden bereit, die die charakteristische Einfachheit von echten konvergierten Infrastrukturen und gleichzeitig mehr Auswahlmöglichkeiten bei den einzelnen Stapelkomponenten erreichen möchten.

VSPEX Proven Infrastructures, wie in Abbildung 1 gezeigt, sind modulare und virtualisierte Infrastrukturen, die von EMC validiert und von EMC VSPEX-Partnern geliefert werden. Sie umfassen die Virtualisierungs-, Server-, Netzwerk-, Speicher- und Datensicherheitsebene. Partner können die Virtualisierungs-, Server- und Netzwerktechnologien auswählen, die am besten zur Umgebung eines Kunden passen. Gleichzeitig stellen die Speichersysteme der hochverfügbaren EMC VNX-Produktreihe und EMC Data Protection-Technologien die Speicher- und Datensicherheitsebene zur Verfügung.

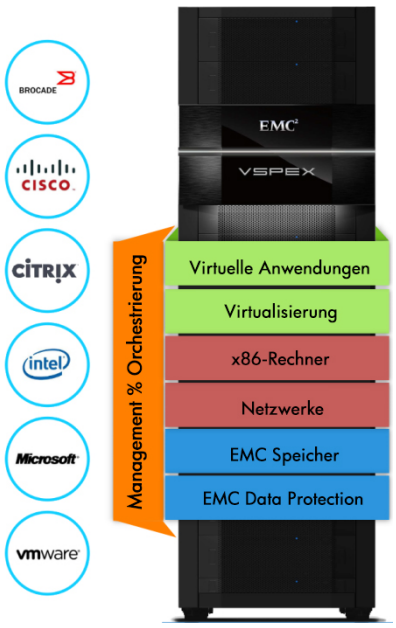


**Abbildung 1. VSPEX Proven Infrastructures**

## Lösungsarchitektur

### Allgemeine Architektur

Die Lösung EMC VSPEX für Anwender-Computing für VMware Horizon View umfasst eine vollständige Systemarchitektur, die bis zu 2.000 virtuelle Desktops unterstützen kann. Die Validierung der Infrastruktur erfolgt an 3 Skalierungspunkten bei 500, 1.000 und 2.000 virtuellen Desktops. Die Lösung unterstützt 2 Arten von Speichertypen: Block und File.

Abbildung 2 zeigt die allgemeine Architektur der validierten Lösung.

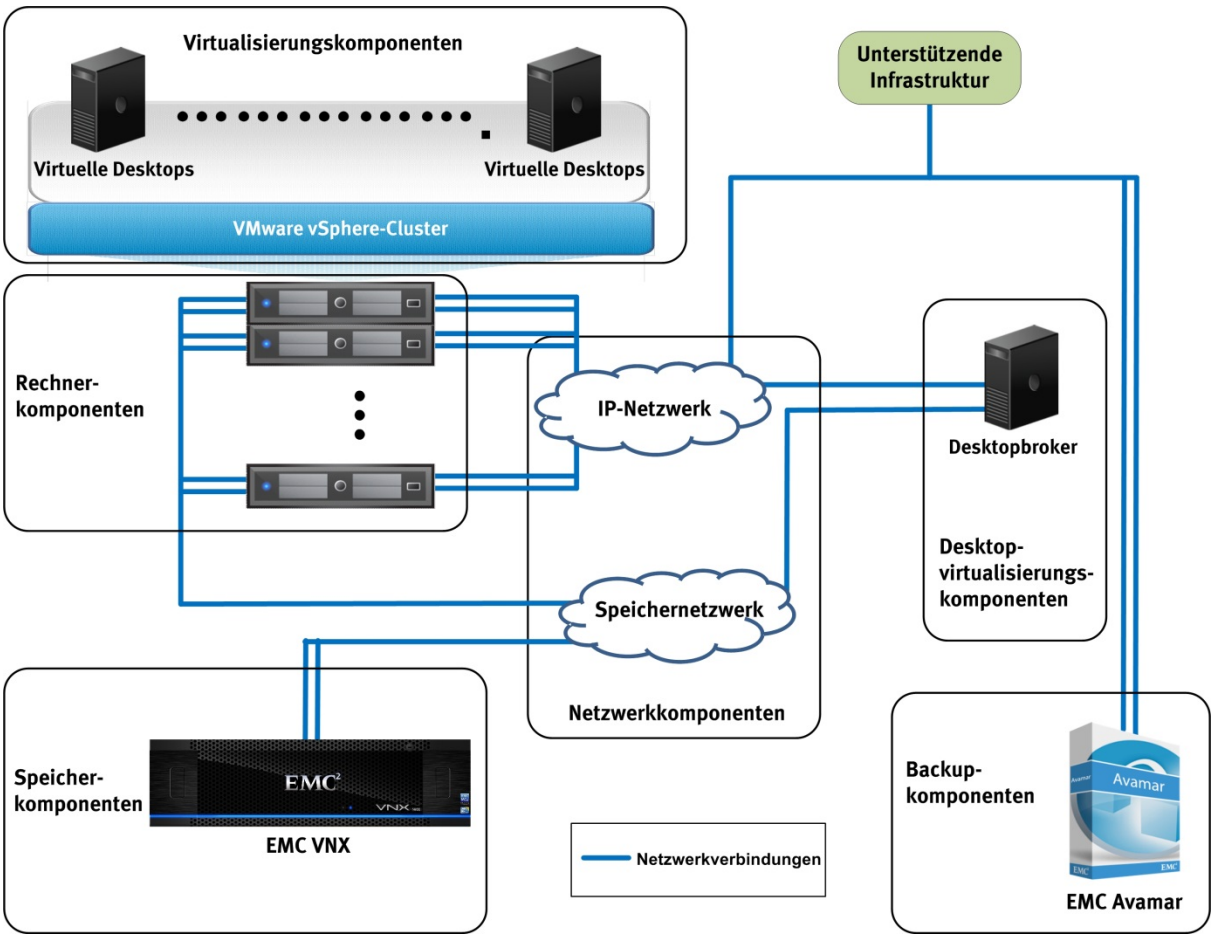


**Abbildung 2. Architektur der validierten Lösung**

Diese Lösung verwendet EMC VNX und VMware vSphere für die Bereitstellung der Speicher- und Virtualisierungsplattformen für eine VMware Horizon View-Umgebung mit virtuellen, von VMware Horizon View Composer bereitgestellten Microsoft Windows 7-Desktops.

Für die Lösung wurde[2] Folgendes bereitgestellt: VNX5200 zur Unterstützung von bis zu 500 virtuellen Desktops, VNX5400 zur Unterstützung von bis zu 1.000 virtuellen Desktops und VNX5600 zur Unterstützung von bis zu 2.000 virtuellen Desktops.

Diese Lösung wird auf einer VSPEX Private Cloud für VMware vSphere ausgeführt und von der hochverfügbaren EMC VNX-Produktreihe unterstützt. Die Infrastrukturservices für die Lösung, die in Abbildung 3 dargestellt sind, können durch eine vorhandene Infrastruktur am Kundenstandort, durch die VSPEX Private Cloud oder durch die Bereitstellung der Services als dedizierte Ressourcen im Rahmen der Lösung bereitgestellt werden.

[2] In diesem Leitfaden bezieht sich „wir“ auf das EMC Solutions Engineering-Team, das die Lösung validierte.

Die Planung und das Design der Speicherinfrastruktur für die Horizon View-Umgebung sind ein wichtiger Schritt, da der gemeinsame Speicher in der Lage sein muss, große Belastungsspitzen bei I/O-Vorgängen abzufangen, die im Laufe eines Tags auftreten. Diese Belastungsspitzen können zu Phasen mit einer unregelmäßigen und unzuverlässigen Performance der virtuellen Desktops führen. Benutzer mögen sich an eine langsame Performance gewöhnen, aber eine unzuverlässige Performance führt zu Frustration und verringert die Effizienz.

Für eine zuverlässige Performance einer Anwender-Computing-Lösung muss das Speichersystem die Spitzen-I/O-Last der Clients bei minimaler Antwortzeit verarbeiten können. Da die Bereitstellung vieler Laufwerke zur Verarbeitung kurzer Zeiträume mit extremen I/O-Belastungen kostspielig ist, wird in dieser Lösung EMC VNX FAST™ Cache verwendet, um die Anzahl der erforderlichen Laufwerke zu reduzieren.

EMC Data Protection-Lösungen ermöglichen den Schutz von Anwenderdaten und die Wiederherstellbarkeit durch Anwender. Dafür werden in dieser Horizon View-Lösung EMC Avamar und der damit verbundene Desktopclient verwendet.

## Logische Architektur

Die EMC VSPEX-Anwender-Computing-Lösung für VMware Horizon View umfasst 2 Arten von Speichervarianten: Block und File. Abbildung 3 zeigt die logische Architektur der Lösung für beide Varianten.

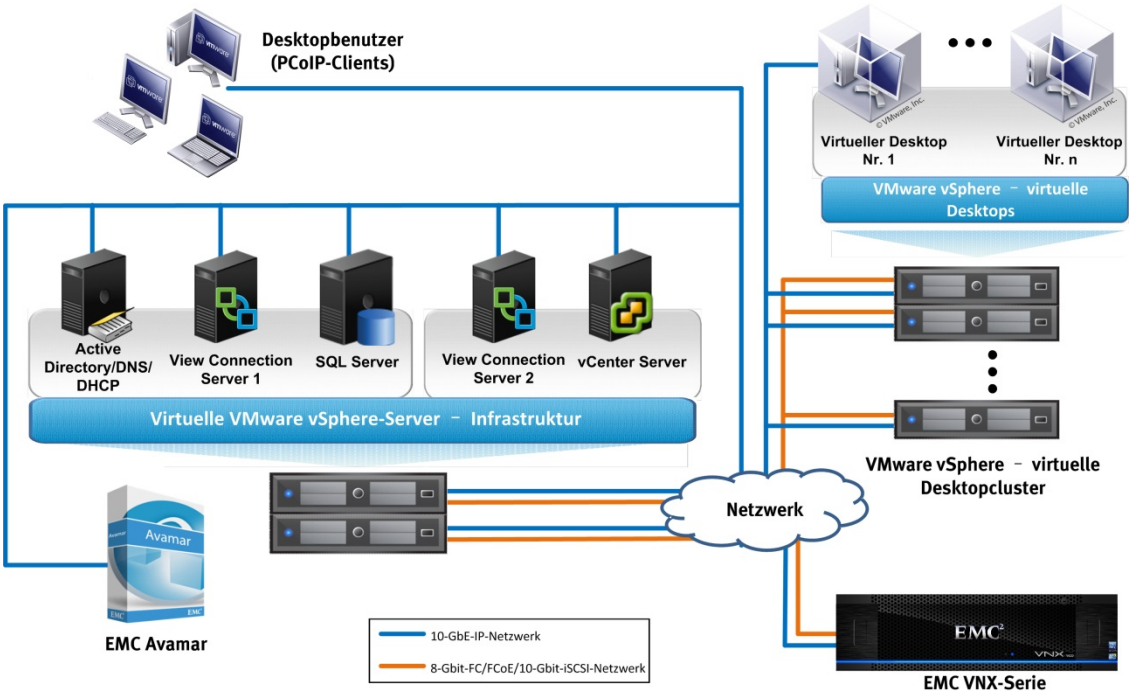


**Abbildung 3. Logische Architektur für Block- und File-basierten Speicher**

Die Blockvariante verwendet 2 Netzwerke: ein Speichernetzwerk zur Bereitstellung von virtuellen Desktop- und virtuellen Serverbetriebssystemdaten sowie ein 10-Gbit-Ethernetnetzwerk für den übrigen Datenverkehr. Für das Speichernetzwerk wird 8-Gbit-FC, 10-Gbit-CEE mit FCoE oder 10-Gbit-Ethernet mit iSCSI-Protokoll verwendet. Die File-basierte Variante nutzt ein 10 GbE-IP-Netzwerk für den gesamten Datenverkehr.

**Hinweis**: Die Lösung unterstützt darüber hinaus 1-Gbit-Ethernet, falls die Bandbreitenerfordernisse erfüllt werden.

# Übersicht über die Kernkomponenten

Tabelle 5 fasst die in dieser Lösung verwendeten Kerntechnologien zusammen. Der Designleitfaden bietet einen Überblick über die einzelnen Komponenten.

**Tabelle 5. Lösungskomponenten**

| VSPEX-Ebene | Komponenten |
|---|---|
| Anwendungsebene | VMware Horizon 6.0 mit View-Desktopvirtualisierungsbroker mit:<br>• View Manager<br>• View Composer<br>• View Persona Management<br>• VMware Horizon View Storage Accelerator<br>• VMware vCenter Operations Manager for Horizon View<br>• VMware Horizon Workspace |
| Virtualisierungsebene | VMware vSphere-Hypervisor mit:<br>• VMware vSphere<br>• VMware vCenter Server<br>• VMware vSphere High Availability<br>• vShield Endpoint |
| Rechnerebene | VSPEX definiert die Mindestanzahl der auf der Rechnerebene benötigten Ressourcen und gibt dem Benutzer die Möglichkeit, diese auf jeder Serverhardware zu implementieren, die diese Anforderungen erfüllt. |
| Netzwerkebene | VSPEX definiert die Mindestanzahl der für die Lösung benötigten Netzwerkports und stellt allgemeine Richtlinien zur Netzwerkarchitektur zur Verfügung, ermöglicht dem Kunden jedoch die Implementierung der Anforderungen mit jeder beliebigen Netzwerkhardware, die diese Anforderungen erfüllt. |
| Speicherebene | EMC VNX-Serie mit:<br>• EMC Unisphere Management Suite<br>• EMC Virtual Storage Integrator (VSI) für VMware vSphere Web Client<br>• VMware vSphere Storage APIs for Array Integration<br>• VMware vSphere Storage APIs for Storage Awareness<br>• EMC VNX Snapshots<br>• EMC SnapSure™<br>• EMC VNX Virtual Provisioning<br>• EMC FAST Suite: FAST Cache und FAST VP (Fully Automated Storage Tiering for Virtual Pools) |
| Datensicherheitsebene | EMC Avamar |
| Sicherheitsschicht | RSA SecurID |

# Kapitel 4 Lösungsimplementierung

In diesem Kapitel werden die folgenden Themen behandelt:

**Übersicht** ..... 26

**Netzwerkimplementierung** ..... 27

**Vorbereiten und Konfigurieren des Speicherarrays** ..... 30

**Installieren und Konfigurieren der vSphere-Hosts** ..... 42

**Installieren und Konfigurieren der SQL Server-Datenbank** ..... 44

**Bereitstellen von VMware vCenter Server** ..... 45

**Einrichten von VMware Horizon View Connection Server** ..... 47

**Provisioning von virtuellen Desktops** ..... 50

**Einrichten von EMC Avamar** ..... 52

**Einrichten von VMware vShield Endpoint** ..... 52

**Einrichten von VMware Horizon Workspace** ..... 54

**Einrichten von VMware vCenter Operations Manager for Horizon View** ..... 59

# Übersicht

In diesem Kapitel wird beschrieben, wie die Referenzarchitektur der Anwender-Computing-Lösung implementiert wird. Wenn Sie bereits über eine VSPEX Proven Infrastructure-Umgebung verfügen, können Sie Abschnitte mit den schon abgeschlossenen Schritten für die Implementierung überspringen. Andernfalls finden Sie Informationen zur Konfiguration der erforderlichen Infrastrukturkomponenten in dem unter Grundlegende Dokumente aufgelisteten VSPEX Proven Infrastructure-Leitfaden.

**Hinweis**: Diese Lösung erfordert bestimmte Infrastrukturservices, die in Abbildung 3 dargestellt sind. Diese können durch eine vorhandene Infrastruktur am Kundenstandort, durch eine VSPEX Private Cloud oder durch die Bereitstellung der Services als dedizierte Ressourcen im Rahmen dieser Lösung bereitgestellt werden.

Tabelle 6 listet die Hauptphasen des Prozesses für die Implementierung der Lösung auf und stellt Links zu den relevanten Abschnitten in diesem Kapitel bereit.

**Tabelle 6. Übersicht über den Implementierungsprozess**

| Phase | Beschreibung | Referenz |
|---|---|---|
| 1 | Konfiguration der Switche und Netzwerke und Herstellen einer Verbindung zum Kundennetzwerk | Netzwerkimplementierung |
| 2 | Installieren und Konfigurieren der VNX | Vorbereiten und Konfigurieren des Speicherarrays |
| 3 | Konfigurieren der Datastores der virtuellen Maschinen | Vorbereiten und Konfigurieren des Speicherarrays |
| 4 | Installieren und Konfigurieren der Server | Installieren und Konfigurieren der vSphere-Hosts |
| 5 | Einrichten von SQL Server (verwendet von vCenter und Horizon View) | Installieren und Konfigurieren der SQL Server-Datenbank |
| 6 | Installieren und Konfigurieren von vCenter und des Netzwerks der virtuellen Maschine | Bereitstellen von VMware vCenter Server |
| 7 | Einrichten von View Connection Server | Einrichten von VMware Horizon View Connection Server |
| 8 | Einrichten von EMC Avamar | Einrichten von EMC Avamar |
| 9 | Einrichten von vShield Endpoint | Einrichten von VMware vShield Endpoint |
| 10 | Einrichten von VMware Horizon Workspace | Einrichten von VMware Horizon Workspace |
| 11 | Einrichten von VMware vCenter Operations Manager for Horizon View | Einrichten von VMware vCenter Operations Manager for Horizon View |

# Netzwerkimplementierung

In diesem Abschnitt werden die Anforderungen für die Vorbereitung der Netzwerkinfrastruktur beschrieben, die zum Support dieser Lösung erforderlich ist. Tabelle 7 enthält eine Zusammenfassung der abzuschließenden Aufgaben sowie Referenzen zu weiteren Informationen.

**Tabelle 7. Aufgaben für die Switch- und Netzwerkkonfiguration**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Konfigurieren des Infrastrukturnetzwerks | Konfigurieren Sie das Speicherarray und das vSphere-Hostinfrastrukturnetzwerk. | Konfigurieren des Infrastrukturnetzwerks |
| Konfigurieren der virtuellen LANs | Konfigurieren Sie private und öffentliche virtuelle LANs nach Bedarf. | Konfigurationsleitfaden Ihres Switchanbieters |
| Konfigurieren des Speichernetzwerks (nur FC-Blockvariante) | Konfigurieren Sie die FC/FCoE-Switchports, das Zoning für vSphere-Hosts und das Speicherarray. | • Konfigurieren des Speichernetzwerks (Blockvariante)<br>• Konfigurationsleitfaden Ihres Switchanbieters |
| Vervollständigen der Netzwerkverkabelung | Verbinden Sie die Switchverbindungsports, VNX-Ports und vSphere-Serverports. | Vervollständigen der Netzwerkverkabelung |

## Konfigurieren des Infrastrukturnetzwerks

Das Infrastrukturnetzwerk erfordert redundante Netzwerkverbindungen für jeden vSphere-Host, das Speicherarray, die Switchverbindungsports und die Switch-Uplink-Ports. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Netzwerkbandbreite bereit.

Diese Konfiguration ist unabhängig davon erforderlich, ob die Netzwerkinfrastruktur für die Lösung bereits vorhanden ist oder zusammen mit anderen Komponenten der Lösung bereitgestellt wird.

Abbildung 4 zeigt ein Beispiel einer redundanten Ethernetinfrastruktur für diese Lösung. Hier ist die Nutzung von redundanten Switchen und Verbindungen dargestellt, um dafür zu sorgen, dass kein Single-Point-of-Failure in der Netzwerkverbindung vorhanden ist.

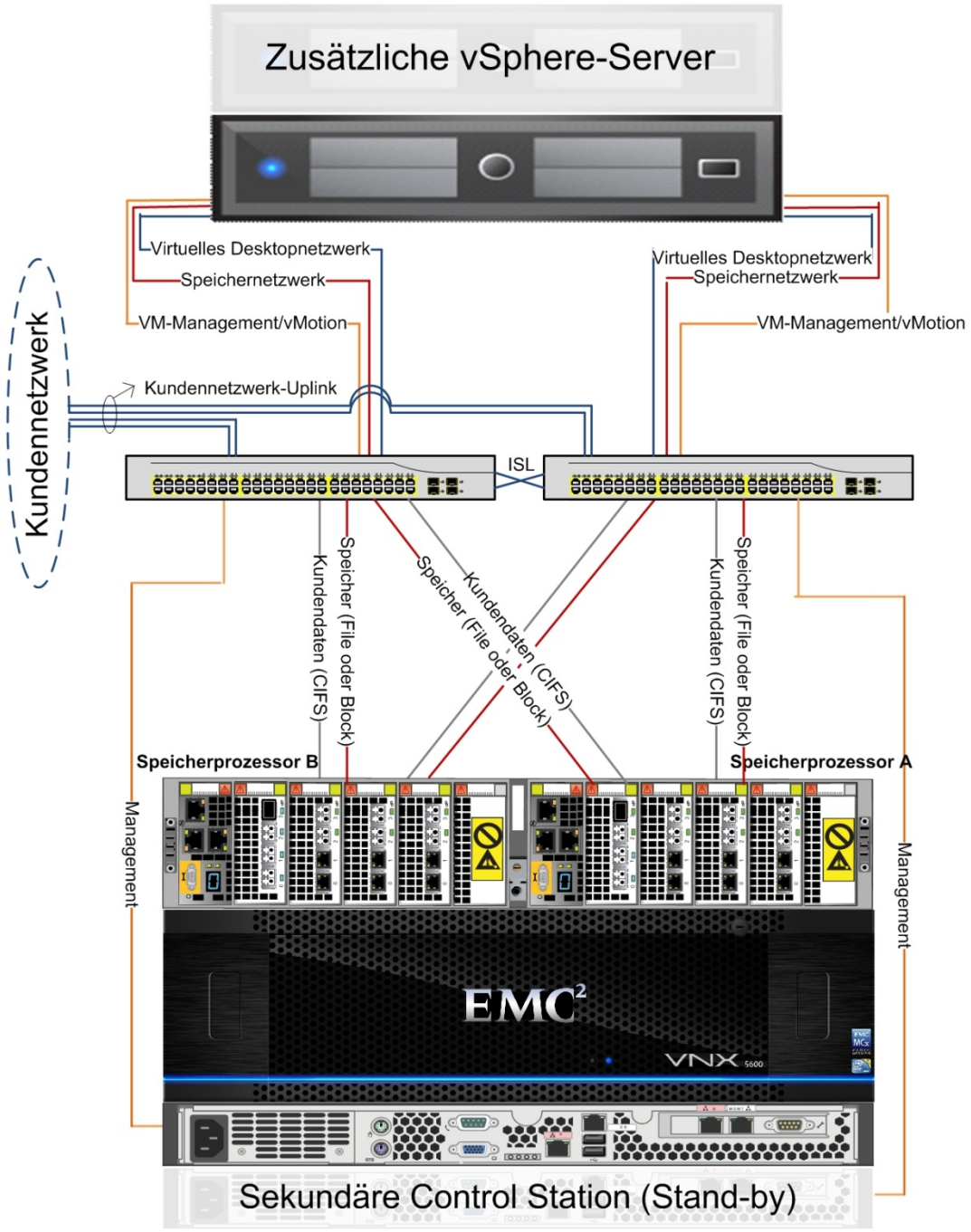


**Abbildung 4. Beispiel-Ethernetnetzwerkarchitektur**

## Konfigurieren der virtuellen LANs

Achten Sie darauf, dass es entsprechende Switchports für das Speicherarray und vSphere-Hosts gibt. EMC empfiehlt, die vSphere-Hosts mit mindestens 3 virtuellen LANs zu konfigurieren:

- **Clientzugriffsnetzwerk**: Netzwerkverbindungen für virtuelle Maschinen und CIFS-Datenverkehr (kundenorientierte Netzwerke, die bei Bedarf getrennt werden können)
- **Speichernetzwerk**: NFS-/iSCSI-/FCoE-Netzwerk (privates Netzwerk)
- **Managementnetzwerk**: vSphere-Management und VMware vMotion (privates Netzwerk)

### Konfigurieren des Speichernetzwerks (Blockvariante)

Für die Blockvariante der Lösung ist ein separates Speichernetzwerk erforderlich. Hier wird ein FC-Netzwerk (Fibre Channel) als Beispiel verwendet. Für das Infrastruktur-Fibre-Channel-Netzwerk sind redundante Fibre-Channel-Switche sowie Links für jeden vSphere-Host und das Speicherarray erforderlich. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Speichernetzwerkbandbreite bereit. Wir haben jeden vSphere-Host mit beiden Fibre-Channel-Switchen und jeden Switch mit jedem Speicherprozessor auf dem Speicherarray verbunden. Wir haben dann jede der Fibre-Channel-Verbindungen zwischen dem vSphere-Host und dem Speicherarray in eine separate Fibre-Channel-Zone platziert.

Abbildung 5 zeigt die Netzwerkarchitektur für dieses Beispiel.

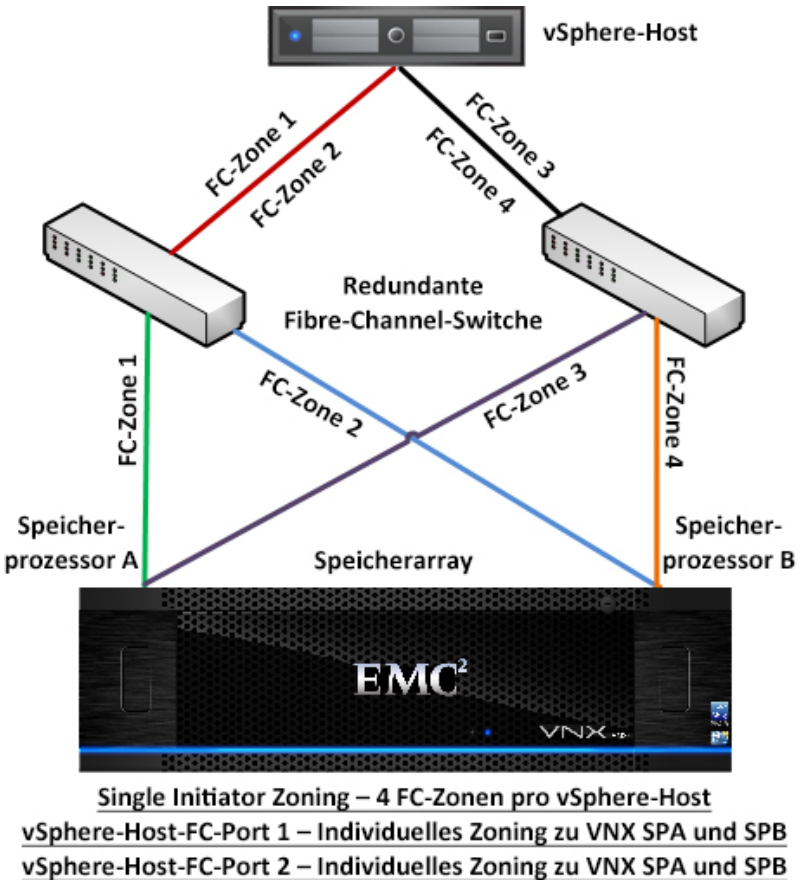


**Abbildung 5. Beispiel für eine Fibre-Channel-Netzwerkarchitektur**

### Vervollständigen der Netzwerkverkabelung

Sorgen Sie dafür, dass alle Lösungsserver, Speicherarrays, Switchverbindungen und Switch-Uplinks über redundante Verbindungen verfügen und in separate Switchinginfrastrukturen eingesteckt sind. Sorgen Sie dafür, dass eine vollständige Verbindung zum vorhandenen Kundennetzwerk vorhanden ist.

**Hinweis**: An diesem Punkt wird die neue Hardware mit dem vorhandenen Kundennetzwerk verbunden. Achten Sie darauf, dass unvorhergesehene Interaktionen keine Serviceprobleme im Kundennetzwerk hervorrufen.

# Vorbereiten und Konfigurieren des Speicherarrays

In diesem Abschnitt wird die Konfiguration des VNX-Speicherarrays beschrieben. In dieser Lösung stellt VNX NFS- oder VMFS-Datenspeicher (VMware Virtual Machine File System) für VMware-Hosts bereit. Tabelle 8 zeigt die Aufgaben für die Speicherkonfiguration.

**Tabelle 8. Aufgaben für die Speicherkonfiguration**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Vorbereiten der VNX | Installieren Sie die VNX-Hardware gemäß der Produktdokumentation. | • VSPEX Private Cloud Proven Infrastructure-Leitfaden |
| Einrichten der anfänglichen VNX-Konfiguration | Konfigurieren Sie die IP-Adressinformationen und andere wichtige Parameter auf der VNX. | • VSPEX Private Cloud Proven Infrastructure-Leitfaden |
| Provisioning von Kerndatenspeicher | Konfigurieren Sie den Kerndatenspeicher so, wie es für die ausgewählte Lösungsvariante und -größe erforderlich ist. | • *Installationshandbuch für VNX5200 Unified*<br>• *Installationshandbuch für VNX5400 Unified*<br>• *Installationshandbuch für VNX5600 Unified*<br>• *Arbeitsblatt für VNX File und Unified*<br>• *Konfigurationsarbeitsblatt für VNX Block*<br>• *Leitfaden für die ersten Schritte mit dem Unisphere-System*<br>• Konfigurationsleitfaden Ihres Switchanbieters<br>• Lösungsdesignleitfaden |
| Provisioning von Speicher für VMFS-Datastores (nur Block) | Erstellen Sie LUNs, die den vSphere-Servern als VMFS-Datastores angezeigt werden, die die virtuellen Desktops hosten. Aktivieren Sie FAST Cache. | |
| Provisioning von Speicher für NFS-Datastores (nur File) | Erstellen Sie NFS-Dateisysteme, die den vSphere-Servern als NFS-Datastores angezeigt werden, die die virtuellen Desktops hosten. Aktivieren Sie FAST Cache. | |
| Provisioning von optionalem Speicher für Benutzerdaten | Erstellen Sie CIFS-Dateisysteme, die zum Speichern von Roamingbenutzerprofilen und Stammverzeichnissen verwendet werden.<br>Konfigurieren Sie optional FAST VP. | |
| Provisioning von optionalem Speicher für virtuelle Infrastrukturmaschinen | Erstellen Sie zusätzliche VMFS-Datastores zum Hosten von Microsoft SQL Server, Domaincontroller, vCenter Server und virtuellen VMware Horizon View Connection Server-Maschinen. | |
| Konfigurieren von Schwellenwerten und Warnmeldungen für Virtual Provisioning | Konfigurieren Sie Schwellenwerte und damit verbundene Warnmeldungen für die Speicherpoolkapazität. | Festlegen von Schwellenwerten und Warnmeldungen für Virtual Provisioning |

### Vorbereiten der VNX

Für diese Lösung gibt es keine spezifischen Konfigurationsschritte. Anweisungen für Zusammenstellung, Rackeinbau, Verkabelung und Stromversorgung für das VNX-Array finden Sie im relevanten VNX-Installationsleitfaden:

- Für bis zu 500 virtuelle Desktops: *EMC VNX5200 Unified – Installationshandbuch*
- Für bis zu 1.000 virtuelle Desktops: *EMC VNX5400 Unified – Installationshandbuch*
- Für bis zu 2.000 virtuelle Desktops: *EMC VNX5600 Unified – Installationshandbuch*

### Einrichten der anfänglichen VNX-Konfiguration

Konfigurieren Sie nach der Vorbereitung des VNX-Arrays wichtige Informationen zur vorhandenen Umgebung, damit das Speicherarray kommunizieren kann. Konfigurieren Sie die folgenden allgemeinen Elemente gemäß den für Ihr IT-Rechenzentrum geltenden Richtlinien und vorhandenen Infrastrukturinformationen.

- Domain Name System (DNS)
- Network Time Protocol (NTP)
- Schnittstellen des Speichernetzwerks
- IP-Adresse des Speichernetzwerks
- CIFS-Services (Common Internet File System) und Active Directory-Domainmitgliedschaft

Weitere Informationen zum Konfigurieren der VNX-Plattform finden Sie in den in Tabelle 8 aufgelisteten Referenzdokumenten. Informationen zum Laufwerkslayout finden Sie im Designleitfaden.

### Provisioning von Kerndatenspeicher

Im Designleitfaden wird das Zielspeicherlayout sowohl für die Block- als auch für die File-basierten Varianten für 500, 1.000 und 2.000 virtuelle Desktops beschrieben.

### Provisioning von Speicher für VMFS-Datastores (nur Block)

Führen Sie die folgenden Schritte in EMC Unisphere aus, um LUNs auf der VNX zu konfigurieren, die zum Speichern der virtuellen Desktops verwendet wird:

1. Erstellen Sie einen blockbasierten RAID-5-Speicherpool mit den in Tabelle 9 gezeigten Merkmalen.

**Tabelle 9. Erstellen eines blockbasierten RAID-5-Speicherpools**

| Konfiguration | Anzahl der Laufwerke | Laufwerkstyp |
|---|---|---|
| 500 virtuelle Desktops | 10 | 300-GB-SAS |
| 1.000 virtuelle Desktops | 15 | 300-GB-SAS |
| 2.000 virtuelle Desktops | 30 | 300-GB-SAS |

a. Melden Sie sich bei Unisphere an.

b. Wählen Sie das Array für diese Lösung aus.

c. Wählen Sie **Storage** › **Storage Configuration** › **Storage Pools**.

d. Klicken Sie auf **Pools**.

e. Klicken Sie auf **Create**.

f. Geben Sie im angezeigten Dialogfeld die Poolparameter an und klicken Sie dann auf **OK.**

g. Stellen Sie sicher, dass FAST Cache im Speicherpool aktiviert ist.

2. Konfigurieren Sie die erforderlichen LUNs aus dem Pool, wie in Tabelle 10 dargestellt, um sie den vSphere-Servern als 4 VMFS-Datastores anzuzeigen.

**Tabelle 10. LUNs auf der VNX zum Speichern virtueller Desktops**

| Konfiguration | Anzahl an LUNs | LUN-Größe (GB) |
|---|---|---|
| 500 virtuelle Desktops | 1 | 50 |
| | 4 | 485 |
| 1.000 virtuelle Desktops | 2 | 50 |
| | 8 | 341 |
| 2.000 virtuelle Desktops | 2 | 50 |
| | 16 | 341 |

a. Wählen Sie **Storage › LUNs** aus.

b. Klicken Sie im angezeigten Dialogfeld auf **Create**.

c. Wählen Sie den in Schritt 1 erstellten Pool aus und geben Sie die LUN-Größe und die Anzahl der bereitzustellenden LUNs an, wie in Tabelle 10 beschrieben.

3. Konfigurieren Sie eine Speichergruppe, damit die vSphere-Server auf die neu erstellten LUNs zugreifen können:

a. Wählen Sie **Hosts › Storage Groups** aus.

b. Erstellen Sie eine neue Speichergruppe.

c. Wählen Sie die LUNs und ESXi-Hosts aus, die dieser Speichergruppe hinzugefügt werden sollen.

### Provisioning von Speicher für NFS-Datastores (nur File)

Führen Sie die folgenden Schritte in Unisphere aus, um NFS-Dateisysteme auf der VNX zu konfigurieren, die zum Speichern der virtuellen Desktops verwendet wird:

1. Erstellen Sie einen blockbasierten RAID-5-Speicherpool mit den in Tabelle 11 gezeigten Merkmalen.

**Tabelle 11. Erstellen eines blockbasierten RAID-5-Speicherpools**

| Konfiguration | Anzahl der Laufwerke | Laufwerkstyp |
|---|---|---|
| 500 virtuelle Desktops | 10 | 300-GB-SAS |
| 1.000 virtuelle Desktops | 15 | 300-GB-SAS |
| 2.000 virtuelle Desktops | 30 | 300-GB-SAS |

a. Melden Sie sich bei Unisphere an.

b. Wählen Sie das VNX-Array für die Lösung aus.

c. Wählen Sie **Storage** › **Storage Configuration** › **Storage Pools**.

d. Klicken Sie auf **Pools**.

e. Klicken Sie auf **Create**.

f. Geben Sie im angezeigten Dialogfeld die Poolparameter an und klicken Sie dann auf **OK.**

g. Stellen Sie sicher, dass FAST Cache für den Pool aktiviert ist.

2. Konfigurieren Sie die erforderlichen LUNs aus dem Pool, wie in Tabelle 12 gezeigt, die dem Data Mover als Dvols eines systemdefinierten NAS-Pools angezeigt werden.

**Tabelle 12. Konfigurieren von LUNs für NAS-Pools**

| Konfiguration | Anzahl an LUNs | LUN-Größe (GB) |
|---|---|---|
| 500 virtuelle Desktops | 10 | 200 |
| 1.000 virtuelle Desktops | 10 | 283 |
| 2.000 virtuelle Desktops | 10 | 566 |

a. Wählen Sie **Storage › LUNs** aus.

b. Klicken Sie auf **Create**.

c. Wählen Sie den in Schritt 1 erstellten Pool aus und geben Sie die Benutzerkapazität und die Anzahl der LUNs an, wie in Tabelle 12 beschrieben.

d. Wählen Sie **Hosts › Storage Groups** aus.

e. Wählen Sie **File Storage** aus.

f. Klicken Sie unter **Available LUNs** auf **Connect LUNs**.

g. Wählen die soeben erstellen 10 LUNs aus.

Sie werden unter **Selected LUNs** angezeigt.

h. Wählen Sie **A new storage pool for file is ready or manually rescan** aus.

i. Wählen Sie **Storage** › **Storage Pool for File** › **Rescan Storage System**, um mehrere Dateisysteme zu erstellen.

---

**Hinweis**: Die Best Practices von EMC Performance Engineering sehen vor, 1 LUN pro 4 Laufwerke im Speicherpool und LUNs in geraden Vielfachen von 10 zu erstellen. Weitere Informationen finden Sie in *EMC VNX Unified: Best Practices für Performance – Leitfaden zur Anwendung von Best Practices*.

---

3. Konfigurieren Sie Dateisysteme aus dem NAS-Pool, wie in Tabelle 13 beschrieben, um sie den vSphere-Servern als 4 NFS-Datastores anzuzeigen.

**Tabelle 13. Konfigurieren von Dateisystemen als NFS-Datastores**

| Konfiguration | Anzahl der Dateisysteme | Dateisystemgröße (GB) |
|---|---|---|
| 500 virtuelle Desktops | 1 | 50 |
| | 4 | 485 |
| 1.000 virtuelle Desktops | 2 | 50 |
| | 8 | 341 |
| 2.000 virtuelle Desktops | 2 | 50 |
| | 16 | 341 |

a. Wählen Sie **Storage** › **Storage Configuration** › **File Systems** aus.

b. Klicken Sie im angezeigten Dialogfeld auf **Create**.

c. Wählen Sie **Create from Storage Pool** aus.

d. Geben Sie im Fenster **Storage Capacity** die erforderliche Anzahl von Dateisystemen an (wie in Tabelle 13 beschrieben) und akzeptieren Sie die Standardwerte für alle anderen Parameter.

4. Exportieren Sie die Dateisysteme mithilfe von NFS und gewähren Sie Root-Zugriff auf die vSphere-Server.

5. Konfigurieren Sie die erforderlichen Data Mover-Parameter:

a. Wählen Sie **Settings** › **Data Mover Parameters**.

b. Wählen Sie in der Liste **Set Parameters** die Option **All Parameters** aus, wie in Abbildung 6 gezeigt.

**Abbildung 6. Anzeigen aller Data Mover-Parameter**

c. Wählen Sie für jeden Data Mover **Properties** aus und aktualisieren Sie **nthreads**, wie in Abbildung 7 gezeigt.

**Hinweis**: Die Standardanzahl von Threads für das Verarbeiten von NFS-Anforderungen liegt bei 384 pro Data Mover auf der VNX. Da bei dieser Lösung mehr als 384 Desktopverbindungen erforderlich sind, sollten Sie die Anzahl der aktiven NFS-Threads auf maximal 512 (für 500 virtuelle Desktops), 1.024 (für 1.000 virtuelle Desktops) oder 2.048 (für 2.000 virtuelle Desktops) pro Data Mover erhöhen.

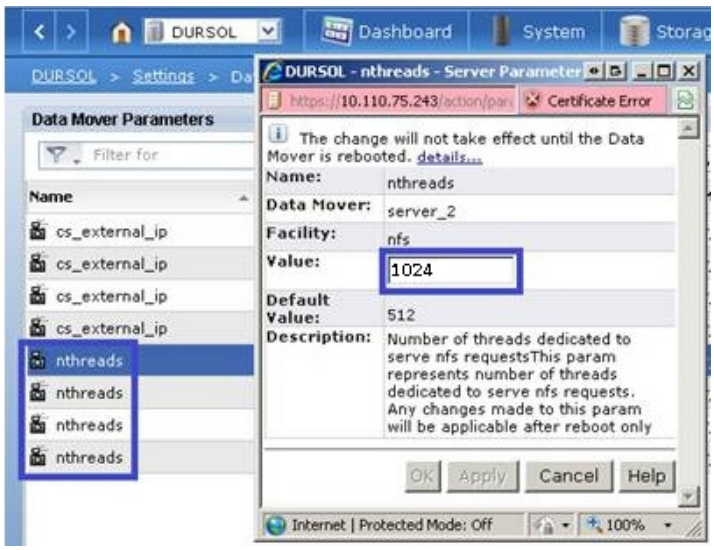


**Abbildung 7. Festlegen von nthread-Parametern**

## Konfigurieren von FAST Cache

Führen Sie in Unisphere die folgenden Schritte aus, um FAST Cache auf dem Speicherpool für diese Lösung zu konfigurieren:

1. So zeigen Sie weitere Informationen zu FAST Cache für das VNX-Array an:
   a. Klicken Sie in Unisphere auf **Properties** und wählen Sie **Manage Cache** aus.
   b. Klicken Sie im Dialogfeld **Storage System Properties** (siehe Abbildung 8) auf **FAST Cache**, um Informationen zu FAST Cache anzuzeigen.

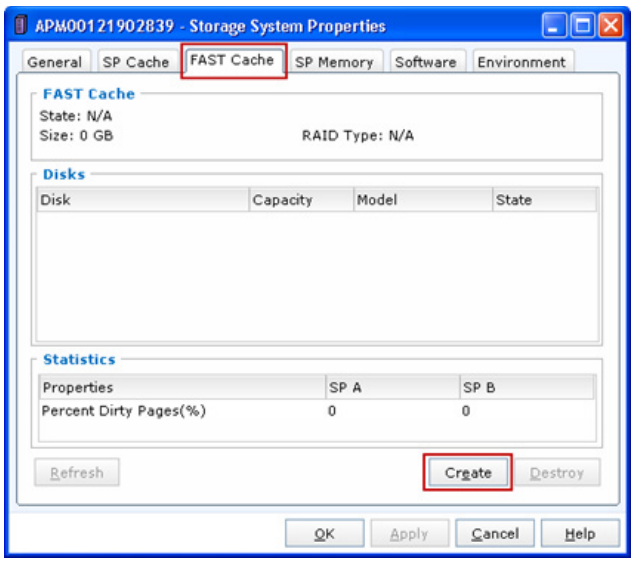


**Abbildung 8. Dialogfeld Storage System Properties**

2. So erstellen Sie FAST Cache:
   a. Klicken Sie auf **Create**, um das Dialogfeld **Create FAST Cache** zu öffnen.

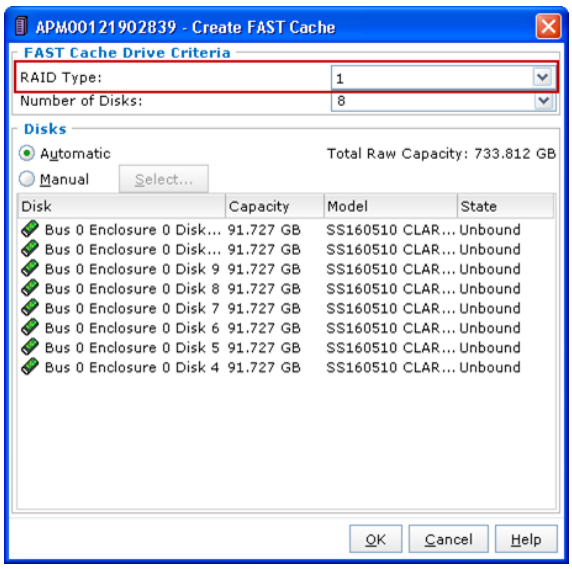
APM00121902839 - Create FAST Cache
FAST Cache Drive Criteria
RAID Type:
1
Number of Disks:
8
Disks
Automatic
Total Raw Capacity: 733.812 GB
Manual
Select...
Disk
Capacity
Model
State
Bus 0 Enclosure 0 Disk... 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk... 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 9 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 8 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 7 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 6 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 5 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 4 91.727 GB SS160510 CLAR... Unbound
OK
Cancel
Help

**Abbildung 9. Dialogfeld Create FAST Cache**

**b.** Wählen Sie die erforderliche Anzahl der Laufwerke aus, die für FAST Cache verwendet werden sollen.

---

**Hinweis**: Informationen zum Bestimmen der in dieser Lösung erforderlichen Anzahl von Flash-Laufwerken finden Sie im Designleitfaden.

---

**c.** Wenn die Option **Automatic** ausgewählt ist, werden die für die Erstellung von FAST Cache verwendeten Flash-Laufwerke im unteren Teil des Dialogfelds angezeigt.

Mit der Option **Manual** können Sie die Laufwerke manuell auswählen.

**d.** Klicken Sie auf **OK**, um FAST Cache mithilfe der ausgewählten Laufwerke zu erstellen.

---

**Hinweis**: Wenn keine ausreichende Anzahl an Flash-Laufwerken verfügbar ist, wird eine Fehlermeldung angezeigt und FAST Cache kann nicht erstellt werden.

---

**e.** Aktivieren Sie FAST Cache für den Speicherpool, der für die Lösung erstellt wurde.

- FAST Cache wird nach der Erstellung standardmäßig für alle neuen Pools aktiviert.
- Um FAST Cache für einen vorhandenen Pool zu aktivieren, wählen Sie im Dialogfeld **Storage Pool Properties** unter **Advanced** die Option **FAST Cache Enabled** aus.

Die FAST Cache-Funktion auf VNX führt nicht zu einer sofortigen Performanceverbesserung. Das System muss Daten zu Zugriffsmustern sammeln und häufig verwendete Informationen in den Cache hochstufen. Dieser Vorgang kann einige Stunden dauern, in denen die Performance des Arrays sich stetig verbessert.

### Provisioning von optionalem Speicher für Benutzerdaten

Wenn in der Produktionsumgebung noch kein für Benutzerdaten (das heißt Roamingbenutzerprofile oder View Persona Management Repositories und Stammverzeichnisse von Benutzern) erforderlicher Speicher vorhanden ist und die optionale Benutzerdatenspindel erworben wurde, führen Sie die folgenden Schritte in Unisphere aus, um 2 CIFS-Dateisysteme auf der VNX zu erstellen:

1. Erstellen Sie einen blockbasierten RAID-6-Speicherpool mit den in Tabelle 14 gezeigten Merkmalen.

**Tabelle 14. Erstellen eines blockbasierten RAID-6-Speicherpools**

| Konfiguration | Anzahl der Laufwerke | Laufwerkstyp |
|---|---|---|
| 500 virtuelle Desktops | 8 | 2-TB-NL-SAS |
| 1.000 virtuelle Desktops | 16 | 2-TB-NL-SAS |
| 2.000 virtuelle Desktops | 32 | 2-TB-NL-SAS |

Im Designleitfaden werden die Speicherlayouts beschrieben.

2. Stellen Sie die erforderlichen LUNs aus dem Pool zur Verfügung, wie in Tabelle 15 gezeigt, die dem Data Mover als Dvols eines systemdefinierten NAS-Pools angezeigt werden.

**Tabelle 15. Konfigurieren von LUNs für NAS-Pools**

| Konfiguration | Anzahl an LUNs | LUN-Größe (TB) |
|---|---|---|
| 500 virtuelle Desktops | 10 | 1 |
| 1.000 virtuelle Desktops | 10 | 1,5 |
| 2.000 virtuelle Desktops | 10 | 3 |

3. Stellen Sie 4 Dateisysteme aus dem NAS-Pool zum Exportieren als CIFS-Shares auf einem CIFS-Server bereit.

## Konfigurieren von FAST VP für Benutzerdaten

Sie können FAST VP optional so konfigurieren, dass die Datenverschiebung zwischen Storage Tiers im Speicherpool für Benutzerdaten automatisiert wird. Sie können FAST VP auf Pool- oder LUN-Ebene konfigurieren.

### Konfigurieren von FAST VP auf Poolebene

Wählen Sie zum Anzeigen und Managen von FAST VP auf Poolebene den Speicherpool für die Benutzerdaten aus und klicken Sie auf **Properties**, um das Dialogfeld **Storage Pool Properties** zu öffnen.

Abbildung 10 zeigt die Tiering-Informationen für einen bestimmten FAST VP-aktivierten Pool.

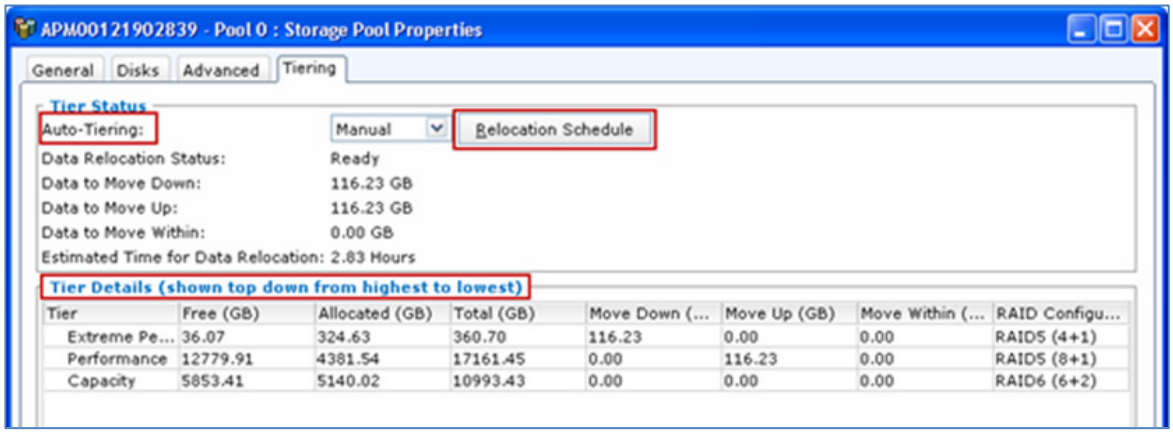


**Abbildung 10. Dialogfeld Storage Pool Properties**

**Tier Status** zeigt FAST-VP-Verlagerungsinformationen an, die für den ausgewählten Pool spezifisch sind. **Tier Details** zeigt die genaue Verteilung der Daten an.

Sie können die geplante Verlagerung auf der Poolebene aus dem Menü **Auto-Tiering** auswählen. Dabei können Sie zwischen den Optionen **Automatic** oder **Manual** auswählen. Klicken Sie auf **Relocation Schedule**, um das Fenster **Manage Auto-Tiering** zu öffnen (siehe Abbildung 11).

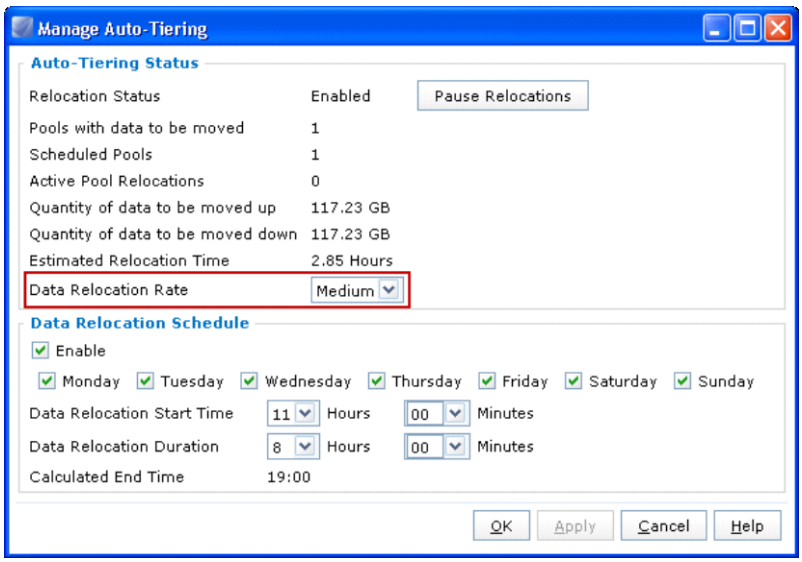


**Abbildung 11. Das Fenster Manage Auto-Tiering**

Über dieses Fenster können Sie die **Data Relocation Rate** steuern. Standardmäßig ist die Rate mit dem Wert **Medium** auf Mittel eingestellt, sodass die Host-I/O-Vorgänge nicht wesentlich beeinträchtigt sind.

---

**Hinweis**: FAST VP ist ein vollständig automatisiertes Tool, d. h. Verlagerungen können automatisch ausgeführt werden. Planen Sie Verlagerungen möglichst außerhalb der Spitzenzeiten, um potenzielle Performanceauswirkungen zu vermeiden.

---

## Konfigurieren von FAST VP auf LUN-Level

Einige FAST VP-Eigenschaften werden auf LUN-Level gemanagt. Klicken Sie mit der rechten Maustaste auf die gewünschte LUN und wählen Sie **Properties**, um das Dialogfeld **LUN Properties** zu öffnen. Klicken Sie in diesem Dialogfeld auf **Tiering**, um Tiering-Informationen für diese LUN anzuzeigen, wie in Abbildung 12 dargestellt.

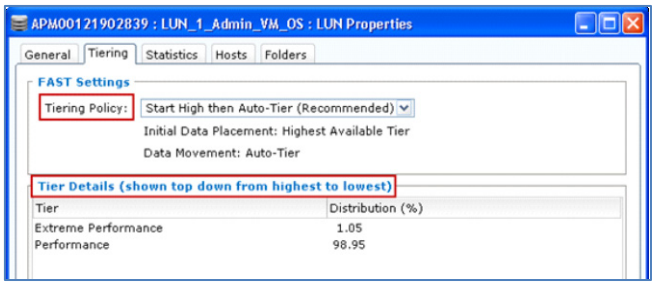


**Abbildung 12. Das Fenster LUN Properties**

Unter **Tier Details** wird die derzeitige Verteilung von Slices innerhalb der LUN angezeigt. Wählen Sie die Tiering Policy für die LUN aus dem Listenfeld **Tiering Policy** aus. Die Standard- und empfohlene Einstellung ist **Start High Then Auto-Tier**.

### Provisioning von optionalem Speicher für virtuelle Infrastrukturmaschinen

Wenn der für virtuelle Infrastrukturmaschinen (das heißt SQL Server, Domaincontroller, vCenter Server bzw. Horizon View View Connection Server) erforderliche Speicher in der Produktionsumgebung noch nicht vorhanden ist und die optionale Benutzerdatenspindel erworben wurde, konfigurieren Sie ein NFS-Dateisystem auf der VNX, das als NFS-Datastore verwendet wird, in dem sich die virtuelle Infrastrukturmaschine befindet. Wiederholen Sie die in Provisioning von Speicher für NFS-Datastores (nur File) gezeigten Konfigurationsschritte, um den optionalen Speicher bereitzustellen und berücksichtigen Sie dabei die kleinere Anzahl von Laufwerken.

### Festlegen von Schwellenwerten und Warnmeldungen für Virtual Provisioning

Abbildung 13 zeigt das Dialogfeld **Storage Pool Properties** in Unisphere, in dem Parameter wie **Total**, **Free**, **Percent Full** und **Total Allocation** für die physische Kapazität eines Systems und **Total Subscription**, **Percent Subscribed** und **Percent Oversubscribed** für die virtuelle Kapazität eines Systems angezeigt werden.

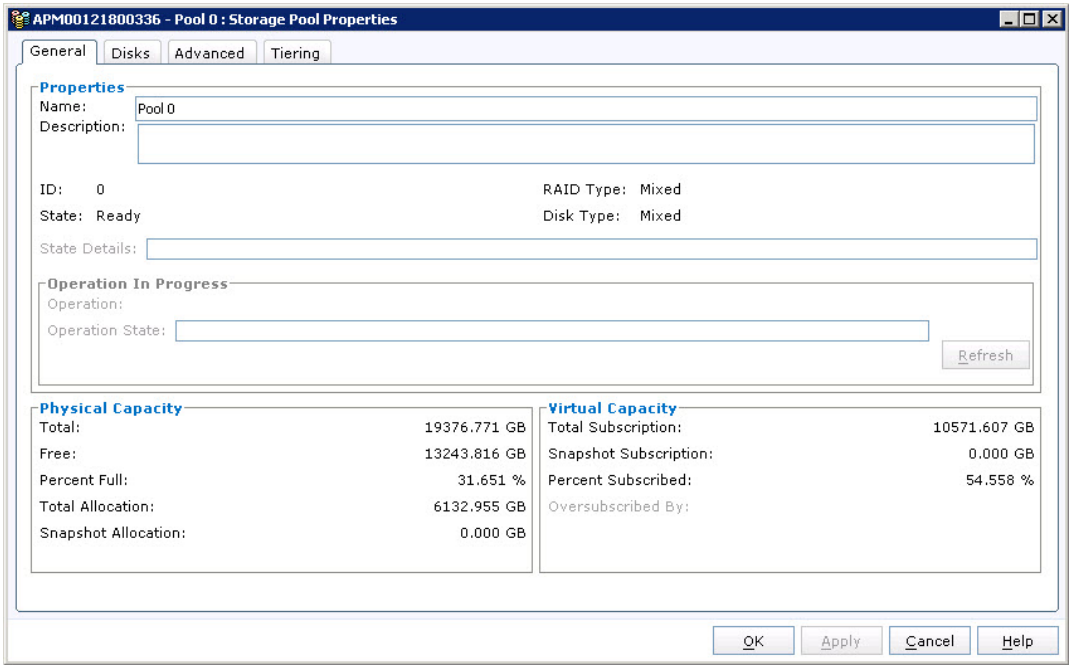


**Abbildung 13. Überprüfen der Speicherplatzauslastung des Speicherpools**

Wenn die Speicherpoolkapazität erschöpft ist, schlagen alle Anforderungen nach zusätzlicher Speicherplatzzuweisung auf bereitgestellten Thin-LUNs fehl. Anwendungen, die versuchen, Daten auf diese LUNs zu schreiben, schlagen in der Regel ebenfalls fehl und es kommt wahrscheinlich zu einem Ausfall. So vermeiden Sie diese Situation:

1. Überwachen Sie die Poolauslastung.
2. Konfigurieren Sie eine Warnmeldung, die Sie bei Erreichen eines Schwellenwerts informiert.
3. Konfigurieren Sie die Option **Percentage Full Threshold** so, dass ausreichend Pufferspeicherplatz vorhanden ist, um einen Ausfall zu verhindern.

   Diese Einstellung finden Sie im Dialogfeld **Storage Pool Properties** unter **Advanced**, wie in Abbildung 14 gezeigt.

**Hinweis**: Diese Warnmeldung ist nur aktiv, wenn es im Pool Thin-LUNs gibt, da Thin-LUNs die einzige Möglichkeit zum Überbelegen eines Pools darstellen. Wenn der Pool nur Thick-LUNs enthält, ist die Warnmeldung nicht aktiv, da kein Risiko besteht, dass der Speicherplatz aufgrund einer Überbelegung ausgeht. Sie können auch den Wert für **Percent Full Threshold** angeben, der **Total Allocation/Total Capacity** entspricht, wenn ein Pool erstellt wird.

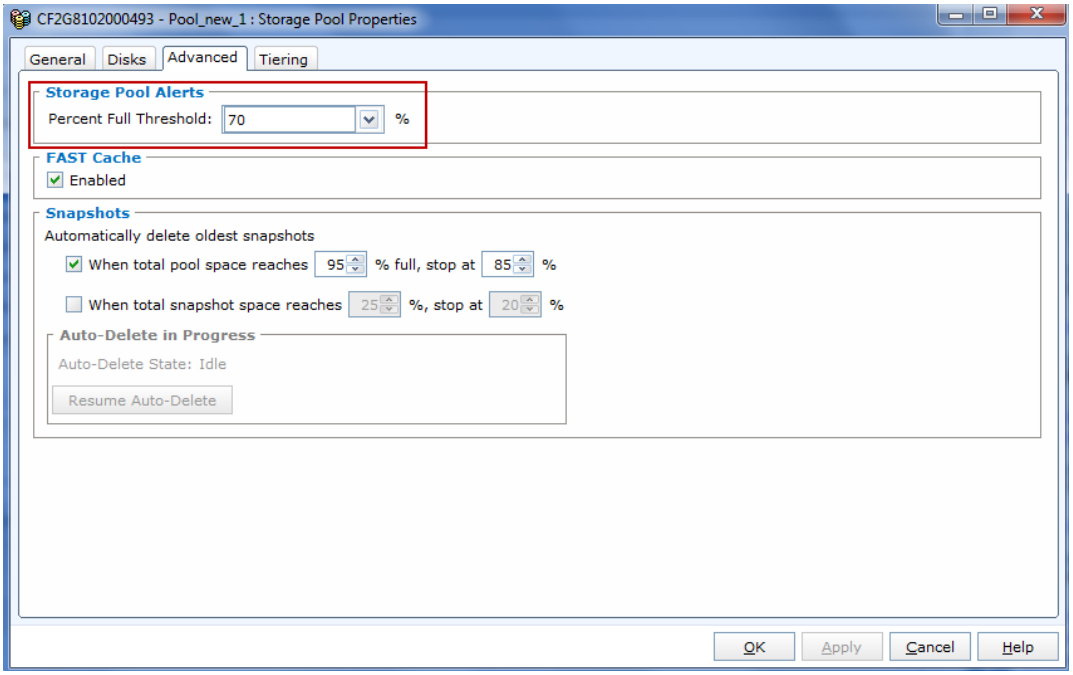


**Abbildung 14. Definieren der Schwellenwerte für die Speicherpoolauslastung**

4. Abbildung 15 zeigt das Fenster **Event Notification**, in dem Sie Warnmeldungen konfigurieren und anzeigen können. Mit dem Konfigurationsassistenten können Sie auch die Option zum Empfang von Warnmeldungen per E-Mail, Paging-Service oder SNMP-Trap auswählen.

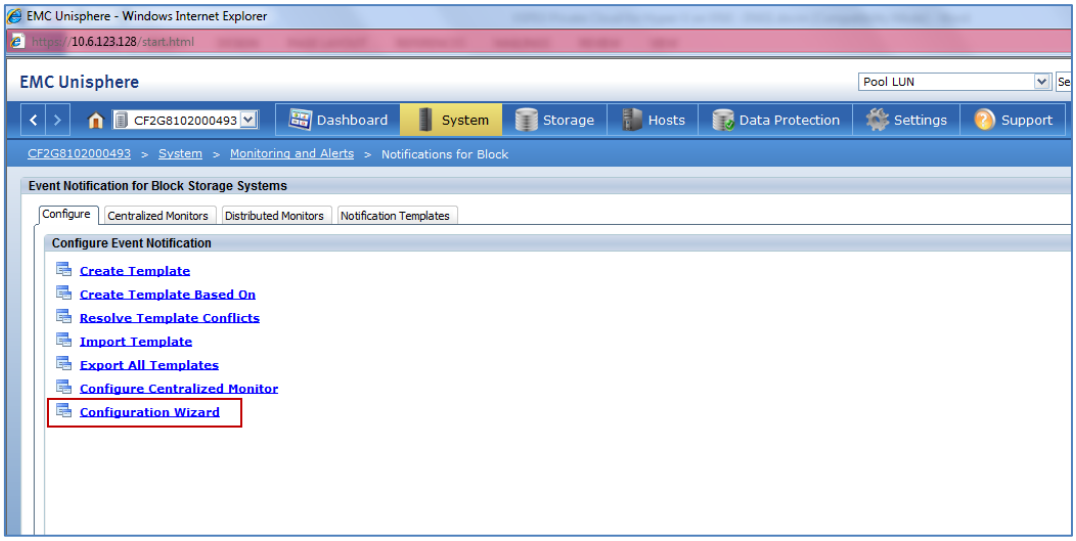


**Abbildung 15. Definieren automatisierter Benachrichtigungen für Block**

Tabelle 16 listet die Informationen zu Schwellenwerten und ihre Einstellungen für VNX Operating Environment (OE) for Block Version 33 auf.

**Tabelle 16. VMX-Schwellenwerte und -Einstellungen**

| Schwellenwerttyp | Schwellenwertbereich | Schwellenwertstandard | Schweregrad der Warnmeldung | Nebeneffekt |
|---|---|---|---|---|
| Vom Benutzer festlegbar | 1 %–84 % | 70 % | Warnung | Ohne |
| Integriert | – | 85 % | Kritisch | Löscht die vom Benutzer festlegbare Warnmeldung |

**Hinweis**: Wenn Sie zulassen, dass die Gesamtzuordnung 90 % der Gesamtkapazität überschreitet, besteht die Gefahr, dass der Speicherplatz ausgeht, was sich auf alle Anwendungen auswirkt, die Thin-LUNs im Pool verwenden.

## Installieren und Konfigurieren der vSphere-Hosts

In diesem Abschnitt finden Sie Informationen zur Installation und Konfiguration der vSphere-Hosts und Infrastrukturserver, die zur Unterstützung der Architektur erforderlich sind. Tabelle 17 beschreibt die Aufgaben, die abgeschlossen werden müssen.

**Tabelle 17. Aufgaben für die Serverinstallation**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Installieren von vSphere | Installieren Sie den vSphere-Hypervisor auf den physischen Servern, die für die Lösung bereitgestellt werden. | *Installations- und Einrichtungshandbuch für vSphere* |
| Konfigurieren des vSphere-Netzwerks | Konfigurieren Sie das vSphere-Netzwerk, einschließlich Trunking von Netzwerkschnittstellenkarten (NICs), VMkernel-Ports, virtuellen Maschinenportgruppen und Jumbo Frames. | *Handbuch für vSphere-Netzwerk* |
| Hinzufügen von vSphere-Hosts zu VNX-Speichergruppen (Blockvariante) | Fügen Sie die vSphere-Hosts den Speichergruppen hinzu, die in Vorbereiten und Konfigurieren des Speicherarrays erstellt wurden. | EMC Online Support |
| Verbinden der VMware-Datastores | Verbinden Sie die VMware-Datastores mit den für die Lösung bereitgestellten vSphere-Hosts. | *Handbuch für vSphere-Speicher* |

### Installieren von vSphere

Bestätigen oder aktivieren Sie nach dem ersten Einschalten der für vSphere verwendeten Server die Einstellung für die hardwaregestützte CPU-Virtualisierung und die hardwaregestützte MMU-Virtualisierung im BIOS des Servers. Wenn die Server mit einem RAID-Controller ausgestattet sind, empfiehlt EMC, eine Spiegelung auf den lokalen Festplatten zu konfigurieren.

Starten Sie die vSphere-Installationsmedien und installieren Sie den Hypervisor auf jedem der Server. Für die Installation sind vSphere-Hostnamen, IP-Adressen und ein Root-Passwort erforderlich. In Arbeitsblatt für die Kundenkonfiguration finden Sie die entsprechenden Werte.

### Konfigurieren des vSphere-Netzwerks

Der VMware *vSphere-Netzwerkleitfaden* beschreibt die vSphere-Netzwerkkonfiguration, einschließlich Lastenausgleich, Linkzusammenfassung und Failover-Optionen. Wählen Sie die entsprechende Option für den Lastenausgleich auf der Basis dessen aus, was von der Netzwerkinfrastruktur unterstützt wird. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

#### Netzwerkschnittstellenkarten

Während der Installation von vSphere wird ein virtueller Standardswitch (vSwitch) erstellt. Standardmäßig wählt vSphere nur eine physische NIC als virtuellen Switch-Uplink aus. Zum Erfüllen der Redundanz- und Bandbreitenanforderungen konfigurieren Sie eine zusätzliche NIC, entweder über die vSphere-Konsole oder durch eine Verbindung mit dem vSphere-Host vom vSphere-Client aus.

Jeder vSphere-Server sollte über mehrere Schnittstellenkarten für jedes virtuelle Netzwerk verfügen, um Redundanz und die Verwendung von Netzwerklastenausgleich, Linkzusammenfassung und Netzwerkadapter-Failover zu ermöglichen.

#### VMKernel-Ports

Erstellen Sie VMkernel-Ports nach Bedarf, basierend auf der Infrastrukturkonfiguration:

- VMkernel-Port für NFS-Datenverkehr (nur File-basierte Variante)
- VMkernel-Port für vMotion
- Virtuelle Desktopportgruppen (verwendet von den virtuellen Desktops für die Kommunikation im Netzwerk)

Im VMware *vSphere-Netzwerkleitfaden* wird das Verfahren für die Konfiguration dieser Einstellungen beschrieben. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

#### Jumbo Frames

Jumbo Frames können auf dem vSphere-Server in 2 verschiedenen Leveln aktiviert werden.

- Wenn alle Portale auf dem virtuellen Switch für Jumbo Frames aktiviert werden sollen, bearbeiten Sie in vCenter die MTU-Einstellungen in vSwitch unter **Properties**.
- Wenn Jumbo Frames für bestimmte VMkernel-Ports aktiviert werden sollen, bearbeiten Sie den VMkernel-Port unter **Network Properties** in vCenter.

So aktivieren Sie Jumbo Frames auf der VNX:

1. Navigieren Sie in Unisphere zu **Settings** › **Network** › **Settings for File**.
2. Wählen Sie die entsprechende Netzwerkschnittstelle unter **Interfaces** aus.
3. Wählen Sie **Properties**.
4. Legen Sie die **MTU-**Größe auf 9.000 fest.
5. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.

Jumbo Frames müssen möglicherweise auch auf jedem Netzwerkswitch aktiviert werden. Anweisungen dazu finden Sie im Konfigurationsleitfaden für Ihren Switch.

### Verbinden der VMware-Datastores

Verbinden Sie die in Vorbereiten und Konfigurieren des Speicherarrays konfigurierten Datastores mit den entsprechenden vSphere-Servern. Dazu zählen die Datastores, die für die folgenden Zwecke konfiguriert wurden:

- Virtueller Desktopspeicher
- Virtueller Infrastrukturmaschinenspeicher (falls erforderlich)
- SQL Server-Speicher (falls erforderlich)

Anweisungen zum Verbinden der VMware-Datastores mit dem vSphere-Host finden Sie im *VMware-Handbuch für vSphere-Speicher*. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

## Installieren und Konfigurieren der SQL Server-Datenbank

Tabelle 18 beschreibt die Aufgaben für die Einrichtung und Konfiguration einer Microsoft SQL Server-Datenbank für die Lösung. Wenn die Aufgaben abgeschlossen sind, ist SQL Server auf einer virtuellen Maschine eingerichtet und alle für vCenter, Update Manager, Horizon View und View Composer erforderlichen Datenbanken sind für die Verwendung konfiguriert.

**Hinweis**: EMC empfiehlt, das Betriebssystem-Volume für die virtuelle SQL Server-Maschine in den Pool der VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind 2 bzw. 6 GB.

**Tabelle 18. Aufgaben für die SQL Server-Datenbankkonfiguration**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Erstellen einer virtuellen Maschine für Microsoft SQL Server | Erstellen Sie eine virtuelle Maschine zum Hosten von SQL Server auf einem der vSphere-Server, der für virtuelle Infrastrukturmaschinen vorgesehen ist und verwenden Sie den für die gemeinsame Infrastruktur bestimmten Datastore.<br>Überprüfen Sie, ob der virtuelle Server die Hardware- und Softwareanforderungen erfüllt. | *vSphere-Administratorhandbuch für virtuelle Maschinen* |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Installieren von Windows | Installieren Sie Microsoft Windows Server 2012 R2 Standard Edition auf der virtuellen Maschine. | *Installieren von Windows Server 2012 R2* |
| Installieren von SQL Server | Installieren Sie Microsoft SQL Server auf der virtuellen Maschine. | *SQL Server-Installation (SQL Server 2012)* |
| Konfigurieren der Datenbank für VMware vCenter Server | Erstellen Sie die für den vCenter Server erforderliche Datenbank auf dem entsprechenden Datastore. | *Vorbereiten der vCenter Server-Datenbanken* |
| Konfigurieren der Datenbank für VMware Update Manager | Erstellen Sie die für Update Manager erforderliche Datenbank auf dem entsprechenden Datastore. | *Vorbereiten der Update Manager-Datenbank* |
| Konfigurieren der Datenbank für VMware Horizon View Composer | Erstellen Sie die für Horizon View Composer erforderliche Datenbank auf dem entsprechenden Datastore. | *Installation von VMware Horizon View* |
| Konfigurieren der Datenbank für VMware Horizon View Manager | Erstellen Sie die für die Horizon View Manager-Eventprotokolle erforderliche Datenbank auf dem entsprechenden Datastore. | *Installation von VMware Horizon View* |
| Konfigurieren der Datenbankberechtigungen für VMware Horizon View und View Composer | Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für die Horizon View- und Horizon View Composer-Datenbanken. | *Installation von VMware Horizon View* |
| Konfigurieren der VMware vCenter-Datenbankberechtigungen | Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für vCenter. | *Vorbereiten der vCenter Server-Datenbanken* |
| Konfigurieren der VMware Update Manager-Datenbankberechtigungen | Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für Update Manager. | *Vorbereiten der Update Manager-Datenbank* |

## Bereitstellen von VMware vCenter Server

Tabelle 19 beschreibt die Aufgaben, die abgeschlossen werden müssen, um VMware vCenter Server für die Lösung zu konfigurieren.

**Hinweis**: EMC empfiehlt, das Betriebssystem-Volume für die virtuelle vCenter Server-Maschine in den Pool der VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind 4 bzw. 8 GB.

**Tabelle 19. Aufgaben für die vCenter-Konfiguration**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Erstellen der virtuellen vCenter-Hostmaschine | Erstellen Sie eine virtuelle Maschine für vCenter Server. | *vSphere-Administratorhandbuch für virtuelle Maschinen* |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Installieren des vCenter-Gastbetriebssystems | Installieren Sie Windows Server 2012 R2 Standard Edition auf der virtuellen vCenter-Hostmaschine. | VMware vSphere-Dokumentation |
| Aktualisieren der virtuellen Maschine | Installieren Sie VMware Tools, aktivieren Sie die Hardwarebeschleunigung und lassen Sie den Remotezugriff auf die Konsole zu. | *vSphere-Administratorhandbuch für virtuelle Maschinen* |
| Erstellen von vCenter ODBC-Verbindungen | Erstellen Sie die 64-Bit vCenter und 32-Bit vCenter Update Manager ODBC-Verbindungen. | • *Installations- und Einrichtungshandbuch für vSphere*<br>• *Installieren und Verwalten von VMware vSphere Update Manager* |
| Installieren von vCenter Server | Installieren Sie die vCenter Server-Software. | *Installations- und Einrichtungshandbuch für vSphere* |
| Installieren von vCenter Update Manager | Installieren Sie die vCenter Update Manager-Software. | *Installieren und Verwalten von VMware vSphere Update Manager* |
| Erstellen eines virtuellen Rechenzentrums | Erstellen Sie ein virtuelles Rechenzentrum. | *Handbuch für vCenter Server- und Hostverwaltung* |
| Anwenden der vSphere-Lizenzschlüssel | Geben Sie die vSphere-Lizenzschlüssel in das vCenter-Lizenzierungsmenü ein. | *Installations- und Einrichtungshandbuch für vSphere* |
| Hinzufügen von vSphere-Hosts | Verbinden Sie den vCenter Server mit den vSphere-Hosts. | *Handbuch für vCenter Server- und Hostverwaltung* |
| Konfigurieren von vSphere-Clustering | Erstellen Sie ein vSphere-Cluster und verschieben Sie die vSphere-Hosts in das Cluster. | *Handbuch zur vSphere-Ressourcenverwaltung* |
| Durchführen der vSphere-Hosterkennung vom Array | Führen Sie die vSphere-Hosterkennung von der Unisphere-Konsole durch. | *Verwenden von EMC VNX-Speicher mit VMware vSphere – TechBook* |
| Installieren des vCenter Update Manager-Plug-ins | Installieren Sie das vCenter Update Manager-Plug-in über die Administrationskonsole. | *Installieren und Verwalten von VMware vSphere Update Manager* |
| Bereitstellen der VAAI-Plug-ins (VMware Storage APIs for Array Integration) | Stellen Sie mithilfe von Update Manager das VAAI-Plug-in für alle vSphere-Hosts bereit. | • *EMC VNX VAAI NFS Plug-in Readme-Datei auf* der EMC Online Support-Website<br>• *Installieren und Verwalten von VMware vSphere Update Manager* |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Bereitstellen von EMC PowerPath/VE (Blockvariante) | Stellen Sie mithilfe von Update Manager das PowerPath/VE-Plug-in für alle vSphere-Hosts bereit. | *Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere* |
| Installation und Konfiguration von EMC VSI für VMware vSphere Web Client OVA-Datei | Verwenden Sie den vSphere-Webclient zum Installieren der VSI für VMware vSphere Web Client OVA-Datei. | *EMC VSI für VMware vSphere Web Client – Produktleitfaden* |
| Installieren von EMC PowerPath Viewer (Blockvariante) | Installieren Sie PowerPath Viewer auf der Administrationskonsole. | *EMC PowerPath Viewer – Installations- und Administrationshandbuch* |

## Einrichten von VMware Horizon View Connection Server

In diesem Abschnitt finden Sie Informationen zum Einrichten und Konfigurieren von VMware Horizon View Connection Server für die Lösung. Für eine Neuinstallation von Horizon View empfiehlt VMware, dass Sie die Aufgaben in der in Tabelle 20 angegebenen Reihenfolge durchführen.

**Hinweis**: EMC empfiehlt, die Betriebssystem-Volumes für die virtuellen View Connection Server-Maschinen in den Pool der VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind 2 bzw. 5 GB.

**Tabelle 20. Aufgaben für die Einrichtung von VMware Horizon View Connection Server**

| Aufgabe | Beschreibung | Referenz | |
|---|---|---|---|
| Erstellen virtueller Maschinen für VMware Horizon View Connection Server | Erstellen Sie 2 virtuelle Maschinen im vSphere-Client. Diese virtuellen Maschinen werden als View Connection Server-Hosts verwendet.<br>Installieren Sie Windows Server 2012 R2 als Gastbetriebssystem für diese Server. | Erstellen virtueller Maschinen für VMware Horizon View Connection Server auf Seite 48 | |
| Installieren von VMware Horizon View Connection Server | Installieren Sie die View Connection Server-Software auf einer der zuvor vorbereiteten virtuellen Maschinen.<br>Geben Sie den View-Lizenzschlüssel in die View Manager-Webkonsole ein. | Installieren von VMware Horizon View Connection Server | *Installation von VMware Horizon View* |
| Konfigurieren der Verbindung zur View-Eventprotokolldatenbank | Konfigurieren Sie die Einstellungen für die View-Eventprotokolldatenbank mithilfe der entsprechenden Datenbankinformationen und Anmeldedaten. | Konfigurieren der Verbindung zur View-Eventprotokolldatenbank auf Seite 48 | |
| Hinzufügen einer Replikatinstanz von View Connection Server | Installieren Sie die VMware View Connection Server-Software auf dem zweiten Server. | Hinzufügen einer Replikatinstanz von View Connection Server auf Seite 48 | |

| Aufgabe | Beschreibung | Referenz | |
|---|---|---|---|
| Konfigurieren der View Composer-ODBC-Verbindung | Konfigurieren Sie entweder auf dem vCenter Server oder einem dedizierten Windows Server 2012 R2-Server eine ODBC-Verbindung für die zuvor konfigurierte View Composer-Datenbank. | Konfigurieren der View Composer-ODBC-Verbindung auf Seite 49 | |
| Installieren von View Composer | Installieren Sie View Composer auf dem im vorherigen Schritt verwendeten Server. | Installieren von View Composer auf Seite 49 | |
| Verbinden von VMware Horizon View mit vCenter und View Composer | Verbinden Sie Horizon View über die View Manager-Webbenutzeroberfläche mit dem vCenter Server und View Composer. | Verbinden von VMware Horizon View mit vCenter und View Composer auf Seite 49 | *VMware Horizon View – Administratorhandbuch* |
| Vorbereiten einer virtuellen Mastermaschine | Erstellen Sie eine virtuelle Mastermaschine als Basis-Image für die virtuellen Desktops. | Vorbereiten einer virtuellen Mastermaschine auf Seite 49 | |
| Konfigurieren von View Persona Management-Gruppen-Policies | Konfigurieren Sie AD-Gruppen-Policies, um View Persona Management zu aktivieren. | Konfigurieren von View Persona Management-Gruppen-Policies auf Seite 50 | |
| Konfigurieren der Gruppen-Policies für die Ordnerumleitung für EMC Avamar | Konfigurieren Sie AD-Gruppen-Policies, um die Ordnerumleitung für Avamar zu aktivieren. | Konfigurieren der Gruppen-Policies für die Ordnerumleitung für EMC Avamar auf Seite 50 | |
| Konfigurieren von View PCoIP-Gruppen-Policies | Konfigurieren Sie AD-Gruppen-Policies für PCoIP-Protokolleinstellungen. | Konfigurieren von View PCoIP-Gruppen-Policies auf Seite 50 | |

**Erstellen virtueller Maschinen für VMware Horizon View Connection Server**

Erstellen Sie im vSphere-Client 2 virtuelle Maschinen, die als View Connection Server-Hosts verwendet werden und installieren Sie Windows Server 2012 R2 als Gastbetriebssystem.

**Installieren von VMware Horizon View Connection Server**

Installieren Sie die View Connection Server-Software gemäß den Anweisungen im Leitfaden *Installation von VMware Horizon View*. Wählen Sie **Standard** aus, wenn Sie aufgefordert werden, den View Connection Server-Typ einzugeben. Geben Sie den View-Lizenzschlüssel in die View Manager-Administrationskonsole ein.

**Konfigurieren der Verbindung zur View-Eventprotokolldatenbank**

Konfigurieren Sie die Verbindung zur View-Eventprotokolldatenbank mithilfe des Datenbankservernamens, des Datenbanknamens und der Datenbankanmeldedaten. Spezifische Informationen zum Konfigurieren des Eventprotokolls finden Sie im Leitfaden zur *Installation von VMware Horizon View*.

**Hinzufügen einer Replikatinstanz von View Connection Server**

Wiederholen Sie den Installationsprozess für den View Connection Server auf der zweiten virtuellen Zielmaschine. Wenn Sie aufgefordert werden, den Connection Server-Typ einzugeben, geben Sie **Replica** an. Stellen Sie dann die Horizon View-

Administratoranmeldedaten bereit, um die View-Konfigurationsdaten der ersten Connection Server-Instanz zu replizieren.

**Konfigurieren der View Composer-ODBC-Verbindung**

Erstellen Sie auf dem Server, der den View Composer-Service hostet, eine ODBC-Verbindung für die zuvor konfigurierte View Composer-Datenbank. Spezifische Informationen zum Konfigurieren der ODBC-Verbindung finden Sie im Leitfaden *Installation von VMware Horizon View*.

**Installieren von View Composer**

Installieren Sie die View Composer-Software auf dem Server, der den View Composer-Service hostet. Geben Sie auf Aufforderung während des Installationsprozesses die zuvor konfigurierte ODBC-Verbindung an. Spezifische Informationen zum Konfigurieren der ODBC-Verbindung finden Sie im Leitfaden *Installation von VMware Horizon View*.

**Verbinden von VMware Horizon View mit vCenter und View Composer**

Erstellen Sie mithilfe der Horizon View Manager-Webkonsole die Verbindung zwischen Horizon View und dem vCenter Server und View Composer. Spezifische Informationen zum Erstellen der Verbindungen finden Sie im *VMware Horizon View – Administratorhandbuch*. Wenn die Option zur Verfügung gestellt wird, aktivieren Sie vSphere-Hostcaching (auch als View Storage Accelerator oder Content Based Read Cache bezeichnet) und legen Sie die Cachegröße auf 2 GB fest, die maximal unterstützte Größe.

Sie können darüber hinaus die Option **Reclaim VM disk space** aktivieren. Diese Funktion wird derzeit nur für Windows 8.1-Desktops unterstützt. Wenn Sie **Reclaim VM disk space** aktivieren, müssen Sie einen Blackout-Zeitraum festlegen, während dessen der Vorgang nicht ausgeführt wird. Da der Vorgang nicht zu Spitzenzeiten ausgeführt werden sollte, muss der Blackout-Zeitraum diese Zeiten abdecken. Standardmäßig wird die Speicherplatzrückgewinnung erst dann ausgeführt, wenn mindestens 1 GB zurückgewonnen werden kann. Sie können einen anderen Wert beim Implementieren der Desktoppools festlegen.

**Vorbereiten einer virtuellen Mastermaschine**

Führen Sie die folgenden Schritte aus, um die virtuelle Mastermaschine vorzubereiten:

1. Erstellen Sie mithilfe von vSphere Web Client eine virtuelle Maschine auf Grundlage der Hardwarespezifikationen für VMware Version 9.

   Sie können virtuelle Maschinen mit Version 9 nicht mit dem Softwareclient erstellen. Verwenden Sie dazu den Webclient.

2. Installieren Sie das Windows 8.1-Gastbetriebssystem.
3. Installieren Sie entsprechende Integrationstools wie VMware Tools.
4. Optimieren Sie die Betriebssystemeinstellungen, um zu verhindern, dass unnötige Hintergrundservices irrelevante I/O-Vorgänge erzeugen, die sich negativ auf die allgemeine Performance des Speicherarrays auswirken.

   Ausführliche Informationen finden Sie in den folgenden Dokumenten: *Bereitstellung von virtuellen Microsoft Windows 8-Desktops mit VMware Horizon View – Anwendung von Best Practices* und *Optimierungshandbuch für Windows 8 für VMware Horizon View*.
5. Installieren Sie Drittanbietertools oder -anwendungen wie Microsoft Office, die für Ihre Umgebung relevant sind.
6. Installieren Sie den Avamar Desktop/Laptop-Client.

7. Details finden Sie im *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View*.
8. Installieren Sie den Horizon View-Agent.

**Hinweis**: Wenn Sie die Horizon View Persona Management-Funktion verwenden, installieren Sie zu diesem Zeitpunkt die Persona Management-Komponente des Horizon View-Agent. Achten Sie darauf, dass die Persona Management-Option während der Installation des Horizon View-Agent ausgewählt wird.

### Konfigurieren von View Persona Management-Gruppen-Policies

View Persona Management wird über Active Directory-Gruppen-Policies aktiviert, die der Organisationseinheit zugewiesen werden, die die Computerkonten für den virtuellen Desktop enthält. Die Vorlagen für die View-Gruppen-Policy befinden sich im Verzeichnis **\Program Files\VMware\VMware View\Server\extras\GroupPolicyFiles** auf dem View Connection Server.

### Konfigurieren der Gruppen-Policies für die Ordnerumleitung für EMC Avamar

Aktivieren Sie die Ordnerumleitung über die Active Directory-Gruppen-Policies, die der Organisationseinheit zugewiesen werden, die die Benutzerkonten für den virtuellen Desktop enthält. Die Active Directory-Ordnerumleitung wird (statt der View Persona Management-Ordnerumleitung) verwendet, damit für die Ordner die von der Avamar-Software geforderten Benennungskonsistenzen beibehalten werden. Details finden Sie im *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View*.

### Konfigurieren von View PCoIP-Gruppen-Policies

View PCoIP-Protokolleinstellungen werden über AD-Gruppen-Policies gesteuert, die der Organisationseinheit zugewiesen werden, die die View Connection-Server enthält. Die Vorlagen für die View-Gruppen-Policy sind in der ZIP-Datei des **Horizon View GPO-Bündels gespeichert**. Verwenden Sie die Gruppen-Policy-Vorlage **pcoip.adm**, um die folgenden PCoIP-Protokolleinstellungen festzulegen:

- Maximum Initial Image Quality value: 70
- Maximum Frame Rate value: 24

**Hinweis**: Höhere Bildraten für die PCoIP-Sitzung und eine höhere Bildqualität können sich nachteilig auf die Serverressourcen auswirken.

## Provisioning von virtuellen Desktops

Verwenden Sie View Composer in der Horizon View-Konsole, um Ihre virtuellen Desktops bereitzustellen:

1. Erstellen Sie einen automatisierten Desktoppool.
2. Geben Sie den bevorzugten Wert für die Option **User Assignment** an:
   - **Dedicated**: Benutzer erhalten bei jeder Anmeldung beim Pool denselben Desktop.
   - **Floating**: Benutzer erhalten bei jeder Anmeldung zufällig aus dem Pool ausgewählte Desktops.
3. Geben Sie einen Wert für **View Composer linked clones** an.
4. Geben Sie einen Wert für die **Pool Identification** an.

5. Konfigurieren Sie **Pool Settings** nach Bedarf.
6. Konfigurieren Sie **Provisioning Settings** nach Bedarf.
7. Akzeptieren Sie die Standardwerte für **View Composer Disks** oder bearbeiten Sie die Werte nach Bedarf.

   Wenn View Persona Management verwendet wird, wählen Sie **Do not** redirect Windows profile under **Persistent Disk** aus (siehe Abbildung 16).

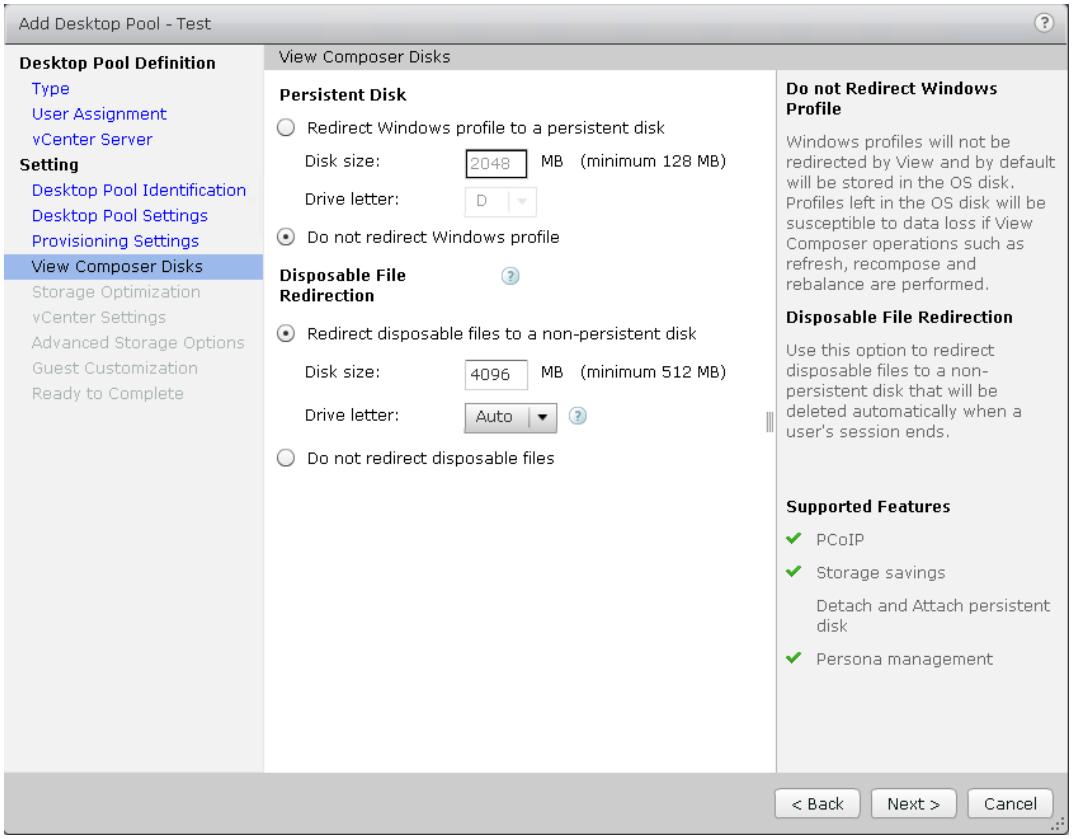
Add Desktop Pool - Test
Desktop Pool Definition
Type
User Assignment
vCenter Server
Setting
Desktop Pool Identification
Desktop Pool Settings
Provisioning Settings
View Composer Disks
Storage Optimization
vCenter Settings
Advanced Storage Options
Guest Customization
Ready to Complete
View Composer Disks
Persistent Disk
Redirect Windows profile to a persistent disk
Disk size: 2048 MB (minimum 128 MB)
Drive letter: D
Do not redirect Windows profile
Disposable File Redirection
Redirect disposable files to a non-persistent disk
Disk size: 4096 MB (minimum 512 MB)
Drive letter: Auto
Do not redirect disposable files
Do not Redirect Windows Profile
Windows profiles will not be redirected by View and by default will be stored in the OS disk. Profiles left in the OS disk will be susceptible to data loss if View Composer operations such as refresh, recompose and rebalance are performed.
Disposable File Redirection
Use this option to redirect disposable files to a non-persistent disk that will be deleted automatically when a user's session ends.
Supported Features
PCoIP
Storage savings
Detach and Attach persistent disk
Persona management
< Back
Next >
Cancel

**Abbildung 16. Das Fenster View Composer Disks**

8. Konfigurieren Sie die AD-Gruppen-Policy für View Persona Management.
9. Wählen Sie **Select separate datastores for replica and OS disk** aus.
10. Wählen Sie die entsprechende übergeordnete virtuelle Maschine, den virtuellen Maschinen-Snapshot, den Ordner, die vSphere-Hosts oder -Cluster, den vSphere-Ressourcenpool sowie die Datastores von verknüpften Clones und Laufwerkreplikaten aus.
11. Aktivieren Sie Hostcaching für den Desktoppool und geben Sie Blackout-Zeiten für die Cacheregeneration an.
12. Geben Sie Image-Anpassungsoptionen nach Bedarf an.
13. Schließen Sie den Poolerstellungsprozess ab, um die Erstellung des virtuellen Desktoppools zu initiieren.

## Einrichten von EMC Avamar

Wenn Ihre Lösung Avamar Data Protection umfasst, beachten Sie die detaillierten Informationen zur Implementierung der Data Protection-Lösung im *Design- und Implementierungsleitfaden: EMC Backup und Recovery für VSPEX für Anwender-Computing für VMware Horizon View*.

## Einrichten von VMware vShield Endpoint

In diesem Abschnitt werden Informationen zum Einrichten und Konfigurieren der Komponenten von vShield Endpoint bereitgestellt. Tabelle 21 beschreibt die Aufgaben, die abgeschlossen werden müssen.

**Hinweis**: EMC empfiehlt, das Betriebssystem-Volume für VMware vShield Endpoint in den Pool der VSPEX Private Cloud zu integrieren. Weitere Informationen zur empfohlenen CPU- und Arbeitsspeicherkonfiguration finden Sie in der *vShield – Kurzanleitung*.

**Tabelle 21. Für die Installation und Konfiguration von vShield Endpoint erforderliche Aufgaben**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Überprüfen der Desktoptreiberinstallation für vShield Endpoint | Überprüfen Sie, ob die vShield Endpoint-Treiberkomponente von VMware Tools auf dem virtuellen Desktopmaster-Image installiert wurde. | *vShield-Kurzanleitung* |
| Bereitstellen der vShield Manager-Appliance | Führen Sie die Bereitstellung und Konfiguration der vShield Manager-Appliance durch. | |
| Registrieren des vShield Manager-Plug-ins | Registrieren Sie das vShield Manager-Plug-in beim vSphere-Client. | |
| Anwenden von vShield Endpoint-Lizenzen | Wenden Sie die vShield Endpoint-Lizenzschlüssel über das vCenter-Lizenzdienstprogramm an. | |
| Installieren des vShield Endpoint-Service | Installieren Sie den vShield Endpoint-Service auf den vSphere-Desktophosts. | |
| Bereitstellen eines Managementservers für die Virenschutzlösung | Führen Sie die Bereitstellung und Konfiguration eines Managementservers für die Virenschutzlösung durch. | *vShield-Kurzanleitung*<br>**Hinweis**: Die Management-Serversoftware für die Virenschutzlösung und virtuellen Sicherheitsmaschinen werden von vShield Endpoint-Partnern bereitgestellt. Genaue Details zur Installation und Konfiguration finden Sie in der Dokumentation des Anbieters. |
| Bereitstellen der virtuellen vSphere-Sicherheitsmaschinen | Führen Sie die Bereitstellung und Konfiguration der virtuellen Sicherheitsmaschinen (SVMs) auf jedem vSphere-Desktophost durch. | |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Überprüfen der vShield Endpoint-Funktion | Überprüfen Sie die Funktion der vShield Endpoint-Komponenten mithilfe des virtuellen Desktopmaster-Image. | **Hinweis**: Details zur Überprüfung der vShield Endpoint-Integration und -Funktion finden Sie in der Dokumentation des Anbieters. |

### Überprüfen der Desktoptreiberinstallation für vShield Endpoint

Der vShield Endpoint-Treiber ist eine Subkomponente des VMware Tools-Softwarepakets, das auf dem virtuellen Desktopmaster-Image installiert ist. Der Treiber wird mit einer von 2 Methoden installiert:

- Wählen Sie während der VMware Tools-Installation **Complete** aus.
- Wählen Sie während der VMware Tools-Installation **Custom** aus. Wählen Sie im Listenfeld VMware **Device Drivers VMCI Driver** und dann **vShield Driver** aus.

Zum Installieren des vShield Endpoint-Treibers auf einer virtuellen Maschine, auf der VMware Tools bereits installiert ist, initiieren Sie die VMware Tools-Installation und wählen Sie die entsprechende Option aus.

### Bereitstellen der vShield Manager-Appliance

Die vShield Manager-Appliance wird von VMware als OVA-Datei bereitgestellt, die über den vShield-Client mithilfe von **File – Deploy OVF template** importiert wird. Die vShield Manager-Appliance ist mit allen erforderlichen Komponenten vorkonfiguriert.

### Installieren des vShield Endpoint-Service

Der vShield Endpoint-Service muss auf allen virtuellen vSphere-Desktophosts installiert sein. Der Service wird auf den vSphere-Hosts von der vShield Manager-Appliance installiert. Die vShield Manager-Webkonsole wird für die Initiierung der vShield Endpoint-Serviceinstallation und zur Überprüfung der erfolgreichen Installation verwendet.

### Bereitstellen eines Managementservers für die Virenschutzlösung

Der Managementserver für die Virenschutzlösung wird für das Management der Virenschutzlösung verwendet und von vShield Endpoint-Partnern bereitgestellt. Der Managementserver und damit verbundene Komponenten sind eine erforderliche Komponente der vShield Endpoint-Plattform.

### Bereitstellen der virtuellen vSphere-Sicherheitsmaschinen

Die virtuellen vSphere-Sicherheitsmaschinen werden von den vShield Endpoint-Partnern bereitgestellt und auf jedem virtuellen vSphere-Desktophost installiert. Die virtuellen Sicherheitsmaschinen führen sicherheitsrelevante Vorgänge für alle virtuellen Desktops aus, die sich auf ihrem vSphere-Host befinden. Die virtuellen Sicherheitsmaschinen und damit verbundene Komponenten sind erforderliche Komponenten der vShield Endpoint-Plattform.

### Überprüfen der vShield Endpoint-Funktion

Nachdem alle erforderlichen Komponenten der vShield Endpoint-Plattform installiert und konfiguriert wurden, sollte die Funktion der Plattform vor der Bereitstellung der virtuellen Desktops überprüft werden.

Überprüfen Sie mithilfe der vom vShield Endpoint-Partner bereitgestellten Dokumentation die Funktion der vShield Endpoint-Plattform mit dem virtuellen Desktopmaster-Image.

# Einrichten von VMware Horizon Workspace

In diesem Abschnitt finden Sie Informationen zur Einrichtung und Konfiguration von VMware Horizon Workspace für die Lösung. Für eine Neuinstallation von Horizon Workspace empfiehlt VMware, dass Sie die Aufgaben in der in Tabelle 22 angegebenen Reihenfolge durchführen.

Zusätzlich zu den Referenzen, die in diesem Abschnitt enthalten sind, bietet die VMware Horizon Workspace-Dokumentation die zusätzlichen Informationen, die erforderlich sind, um die Installation und Konfiguration der VMware Horizon Workspace abzuschließen.

**Hinweis**: EMC empfiehlt, die Horizon Workspace vApp in den Pool der VSPEX Private Cloud zu integrieren.

**Tabelle 22. Aufgaben beim Einrichten von VMware Horizon Workspace**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen | Für jede virtuelle Horizon Workspace-Appliance ist eine IP-Adresse erforderlich. | Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen auf Seite 57 |
| Gewähren der SMTP-Relayberechtigungen für Workspace | Horizon Workspace muss SMTP-Nachrichten bezüglich Benutzerkontoinformationen und Warnmeldungen senden können. | • Gewähren der SMTP-Relayberechtigungen für Workspace auf Seite 57<br>• E-Mail-Serverdokumentation |
| Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für Workspace | Horizon Workspace speichert wichtige Konfigurationsinformationen in einer Datenbank. Eine externe Datenbank wird aus Performance- und Skalierungsgründen empfohlen. | Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für Workspace auf Seite 57 |
| Konfigurieren einer CIFS-Share zur Verwendung als ThinApp-Repository (optional) | Um die Verteilung der Anwendungen, die in VMware ThinApp enthalten sind, zu aktivieren, ist die Dateifreigabe mit Leseberechtigung für Horizon Workspace-Benutzer erforderlich. | • Konfigurieren einer CIFS-Share zur Verwendung als ThinApp-Repository (optional) auf Seite 57<br>• *EMC VNX – Installationshandbuch*<br>• *Leitfaden für die ersten Schritte mit dem Unisphere-System* |
| Überprüfen der angegebenen E-Mail-Adressen aller Workspace-Benutzer | Für Horizon Workspace ist die Angabe von E-Mail-Adressen durch die Benutzer erforderlich. | Überprüfen der angegebenen E-Mail-Adressen aller Workspace-Benutzer auf Seite 58 |
| Bereitstellen der Workspace Portal-Appliance in vCenter | Die Horizon Workspace vApp wird als OVA-Datei bereitgestellt, die die Dateien für die Bereitstellung der Horizon Workspace-Appliance enthält. | Bereitstellen einer Workspace-Appliance in vCenter auf Seite 58 |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Optionales Bereitstellen einer zweiten Workspace-Portal-Appliance in vCenter | In Kombination mit einer Lastenausgleichslösung kann eine zweite Workspace Portal-Appliance für den Lastenausgleich und zum Erzielen einer hohen Verfügbarkeit von Horizon Workspace verwendet werden. | *Erweiterte Konfiguration für die VMware Workspace Portal-Appliance* |
| Erstellen eines Active Directory-Kontos für die Workspace AD-Integration | Dieses Konto wird von Horizon zum Synchronisieren von Active Directory-Kontodaten verwendet und muss sich innerhalb der Organisationseinheit befinden, die die Horizon-Zielbenutzer enthält. | Windows-Dokumentation auf der Microsoft TechNet-Website |
| Erlangen der Informationen, die zum Aktivieren der Workspace-Integration mit Active Directory erforderlich sind | Horizon Workspace muss auf Active Directory zugreifen können, damit Benutzerkonten und AD-Gruppen aufgelöst werden können. | Erlangen der Informationen, die zum Aktivieren der Workspace-Integration mit Active Directory erforderlich sind auf Seite 58 |
| Erstellen eines Active Directory-Kontos für die Workspace vCenter-Integration | Dieses Konto wird von Horizon zur Integration mit dem VMware vCenter Server verwendet. | Anbieterdokumentation |
| Erlangen der Informationen, die zum Aktivieren der Workspace-Integration mit VMware vCenter erforderlich sind | Es werden u. a. folgende Informationen benötigt:<br>vCenter-Hostname-FQDN<br>vCenter-Portnummer<br>Benutzername für das zuvor erstellte Horizon Workspace vCenter-Integrationskonto<br>Passwort für das zuvor erstellte Horizon Workspace vCenter-Integrationskonto | |
| Erlangen des Workspace-Lizenzschlüssels | Der Lizenzschlüssel wird von VMware zur Verfügung gestellt und aktiviert die Horizon Workspace-Plattform. | |
| Verwenden des Webportals für die Workspace-Administration zum Abschließen der webbasierten UI-Installation | Unter https://*workspace-va-FQDN:8443* können Sie auf das Webportal für die Workspace-Administration zugreifen. | |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die virtuelle Workspace-Maschine (optional) | Standardmäßig installiert Workspace ein selbstsigniertes SSL-Zertifikat, dem weder Webclients noch Computer mit der Workspace-Software vertrauen. Das Zertifikat muss ersetzt werden, um diese Fehler zu vermeiden. | Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die Horizon Workspace-Appliance (optional) auf Seite 58 |
| Aktivieren von RSA SecurID-basierter Authentifizierung (optional) | Workspace unterstützt RSA SecurID als Authentifizierungsmechanismus. Greifen Sie auf das Webportal für die Workspace-Administration unter https://*workspace-va-FQDN* zu, um diese Option zu aktivieren. | RSA-Dokumentation |
| Konfigurieren des externen Zugriffs auf die Workspace-Appliance (optional) | Um den externen Zugriff für andere Horizon Workspace-Komponenten zu aktivieren, benötigen Sie externen Zugriff auf die Horizon Workspace-Appliance. | • Konfigurieren des externen Zugriffs auf die Workspace-Appliance (optional) auf Seite 59<br>• Firewallherstellerdokumentation |
| Aktivieren der Horizon View-Integration (optional) | Bei Integration in Horizon View können Horizon Workspace-Benutzer direkt vom Horizon Workspace Portal auf ihre View-Desktops zugreifen. | Aktivieren der Horizon View-Integration (optional) auf Seite 59 |
| Aktivieren von ThinApp-Paketen (optional) | Workspace bietet Ihnen die Möglichkeit, Anwendungen automatisch mithilfe von ThinApp als Pakete für Clients zu verteilen, die den Horizon-Agent ausführen, oder diese Anwendungen on demand an Webclients zu streamen. | • *VMware Workspace Portal – Administratorhandbuch*<br>• *Einrichten von Ressourcen im VMware Workspace Portal*<br>• *VMware Workspace Portal – Benutzerhandbuch* |
| Aktivieren von Webanwendungen (optional) | Workspace umfasst einen Katalog von Webanwendungen, die mit dem Workspace Portal bereitgestellt werden können. | |
| Aktivieren von Citrix-veröffentlichten Anwendungen (optional) | Workspace kann in Citrix XenApp integriert werden, um Zugriff auf Anwendungen, die durch diese Plattform gehostet werden, zu ermöglichen. | |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Benutzern erlauben, Horizon Workspace-Funktionen zu verwenden | Workspace-Benutzer verfügen standardmäßig nicht über die Berechtigung, die Funktionen von Horizon Workspace zu verwenden. Verwenden Sie das Workspace-Dashboard, um Policies zu erstellen und AD-Benutzern und -Gruppen Zugriff auf Workspace-Funktionen zu gewähren. | |
| Erfassen von Anwendungen mithilfe von VMware ThinApp (optional) | Mithilfe von ThinApp erfasste Anwendungen können in das Workspace ThinApp-Repository hochgeladen werden und Clients, die Workspace-Policies verwenden, zur Verfügung gestellt werden. | • *ThinApp – Benutzerhandbuch*<br>• *ThinApp Package.ini-Parameter – Referenzleitfaden* |

### Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen

Die DNS-Datensätze zu den Horizon Workspace-Appliances müssen vor der Bereitstellung mithilfe der gewünschten IP-Adressen der einzelnen Appliances erstellt werden. Sowohl Forward (A)- als auch Reverse (PTR)-Datensätze sollten erstellt werden.

### Gewähren der SMTP-Relayberechtigungen für Workspace

Die Horizon Workspace-Appliance muss dazu in der Lage sein, Nachrichten mit einem SMTP-Server zu übermitteln. Konfigurieren Sie zu diesem Zweck eine vorhandene E-Mail-Adresse und vergewissern Sie sich, dass die Workspace-Appliance die erforderlichen Berechtigungen hat.

### Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für Workspace

Während der Erstkonfiguration von Horizon Workspace werden Sie dazu aufgefordert, die standardmäßige eingebettete PostgreSQL-Datenbank oder eine Datenbank zu verwenden, die auf einem dedizierten Server gehostet wird, auf dem entweder eine unterstützte Version von Oracle oder PostgreSQL ausgeführt wird. Aus Performance- und Managementgründen empfiehlt EMC die Verwendung eines dedizierten Servers, um die Horizon Workspace-Datenbank zu hosten.

Sie müssen diese Datenbank vor der Konfiguration von Horizon Workspace erstellen. Befolgen Sie dazu die Anweisungen im Dokument *Installieren und Konfigurieren von VMware Workspace Portal*. Die Datenbank benötigt 64 GB Speicherplatz und kann Horizon Workspace- Umgebungen mit bis zu 100.000 Benutzern bedienen.

### Konfigurieren einer CIFS-Share zur Verwendung als ThinApp-Repository (optional)

Wenn Sie Horizon Workspace dafür verwenden, Anwendungen bereitzustellen, die mit VMware ThinApp zusammengestellt wurden, erstellen Sie eine CIFS- oder Windows-Share für die Speicherung von Anwendungen. Der Platzbedarf hängt von der Anzahl der Pakete ab, die von der Share gehostet werden.

Wenn Sie VNX zum Hosten der ThinApp-Share verwenden, erstellen Sie das erforderliche Dateisystem innerhalb des Infrastrukturserver-Speicherpools und erstellen Sie dann eine CIFS-Share. Horizon Workspace-Benutzer benötigen schreibgeschützten Zugriff auf diese Share, während für ThinApp-Administratoren zum Verwalten der ThinApp-Pakete Lese-/Schreibzugriff erforderlich ist.

**Überprüfen der angegebenen E-Mail-Adressen aller Workspace-Benutzer**

In Horizon Workspace müssen alle Benutzer eine E-Mail-Adresse in ihrem Active Directory-Konto angeben. Wenn das E-Mail-Adressfeld in Active Directory leer ist, wird Horizon Workspace nicht für den betreffenden Benutzer aktiviert.

Das AD-Konto muss nicht E-Mail-fähig sein. Das ist ein Begriff, der für Unternehmen verwendet wird, die Microsoft Exchange verwenden. Nur Horizon Workspace erfordert, dass das E-Mail-Adressfeld des Benutzers in Active Directory eine gültige E-Mail-Adresse enthält.

**Bereitstellen einer Workspace-Appliance in vCenter**

Wenn Sie die **Deploy OVF Template**-Funktion in der vCenter-Konsole verwenden, stellen Sie die Horizon Workspace Portal-Appliance bereit. Legen Sie dazu folgende Feldwerte fest:

- **Host Name (FQDN)**: Vollständig qualifizierter Domainname für die Horizon-Gateway-Appliance
- **Standardgateway**
- **DNS**: AD-Domain DNS-Server. Bei Angabe mehrerer IP-Adressen müssen diese durch ein Komma getrennt werden.
- **IP Address**: IP-Adresse für die Workspace-Appliance
- **Netzmaske**
- **Disk Format**: Thin Provisioning
- **Network Mapping**: Zielnetzwerk für die virtuelle Workspace-Appliance

**Erlangen der Informationen, die zum Aktivieren der Workspace-Integration mit Active Directory erforderlich sind**

Für Horizon Workspace ist es erforderlich, dass die AD-Konten der Benutzer in einer anderen Organisationseinheit (OU) gespeichert sind, als die standardmäßige Benutzerorganisationseinheit, und zwar wie folgt:

- Name des AD-Domaincontrollers und FQDN
- AD-Kontext für die Anbindung; das Stammverzeichnis der AD-Organisationseinheit, die Horizon-Benutzer und -Gruppen enthält, z. B.:

  OU=HorizonWorkspace,DC=rtp,DC=lab,DC=emc,DC=com
- AD-Basis-DN des zuvor erstellten Horizon Workspace AD-Integrationskontos, z. B.:

  CN=svc-horizon,OU=HorizonWorkspace,DC=rtp,DC=lab,DC=emc,DC=com
- Passwort für das zuvor erstellte Horizon Workspace AD-Integrationskonto
- AD-Benutzername und -Passwort eines Kontos mit der Berechtigung, Computer mit der Domain zu verknüpfen

**Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die Horizon Workspace-Appliance (optional)**

Sie können ein vertrauenswürdiges SSL-Zertifikat und einen dazugehörigen privaten Schlüssel verwenden, um das selbstsignierte Standard-SSL-Zertifikat der Horizon Workspace-Appliance zu ersetzen. Wenn das Zertifikat nicht ersetzt wird, können Clients auf SSL-Validierungsfehler stoßen, wenn sie auf die Horizon Workspace-Umgebung zugreifen. Die Stamm- und Zwischenzertifikate sind ebenfalls erforderlich, um den Zertifikataustauschprozess abzuschließen.

Sie können ein einziges Platzhalterzertifikat verwenden oder individuelle Zertifikate auf jeder virtuellen Workspace-Maschine ersetzen. Die Zertifikate sollten das PEM-Format aufweisen.

### Konfigurieren des externen Zugriffs auf die Workspace-Appliance (optional)

Horizon Workspace muss über das Internet erreichbar sein, um Funktionen wie die Nutzung von Horizon Workspace als Gateway für den externen Zugriff auf VMware Horizon View zu ermöglichen.

Wenn diese Funktionen erforderlich sind, konfigurieren Sie den externen Zugriff wie im Dokument *Installieren und Konfigurieren von Horizon Workspace Portal* beschrieben.

### Aktivieren der Horizon View-Integration (optional)

Wenn Horizon Workspace als Gateway für den Zugriff auf VMware Horizon View verwendet wird, müssen die View-Integration in die Horizon Workspace-Konsole sowie die SAML-Authentifizierung in VMware Horizon View aktiviert werden.

## Einrichten von VMware vCenter Operations Manager for Horizon View

In diesem Abschnitt werden Informationen zum Einrichten und Konfigurieren von VMware vCenter Operations Manager for Horizon View bereitgestellt. Tabelle 23 beschreibt die Aufgaben, die abgeschlossen werden müssen.

**Hinweis**: EMC empfiehlt, das Betriebssystem-Volume für den VMware vCenter Operations Manager for Horizon View-Server in den Pool der VSPEX Private Cloud zu verlagern. Weitere Informationen zur empfohlenen CPU- und Speicherkonfiguration finden Sie im *VMware vCenter Operations Manager for Horizon View – Installations- und Konfigurationshandbuch*.

**Tabelle 23. Für die Installation und Konfiguration von vCenter Operations Manager erforderliche Aufgaben**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Erstellen eines vSphere-IP-Pools für vCenter Operations Manager | Erstellen Sie einen IP-Pool mit 2 verfügbaren IP-Adressen für die vCenter Operations Manager-Analysen und virtuellen Maschinen der Benutzeroberfläche. | • *VMware vCenter Operations Manager for Horizon View – Installations- und Konfigurationshandbuch*<br>• *VMware vCenter Operations Manager for Horizon View – Administratorhandbuch*<br>• *VMware vCenter Operations Manager for Horizon View – Sicherheitshandbuch* |
| Bereitstellen von vCenter Operations Manager vSphere Application Services (vApp) | Führen Sie die Bereitstellung und Konfiguration der vCenter Operations Manager vApp durch.<br>Passen Sie die Spezifikationen der 2 virtuellen Server, die vCenter Operations Manager vApp umfassen, abhängig von der Anzahl der überwachten virtuellen Maschinen an. | |
| Angeben des zu überwachenden vCenter-Servers | Geben Sie auf der Hauptweboberfläche von vCenter Operations Manager den Namen des vCenter-Servers an, der die virtuellen Desktops managt. | |

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Zuweisen der vCenter Operations Manager-Lizenz | Wenden Sie die vCenter Operations Manager for Horizon View-Lizenzschlüssel über das vCenter-Lizenzdienstprogramm an. | |
| Konfigurieren der SNMP- und SMTP-Einstellungen | Konfigurieren Sie über die Hauptweboberfläche von vCenter Operations Manager alle für Überwachungszwecke erforderlichen SNMP- oder SMTP-Einstellungen.<br>**Hinweis**: Diese Einstellung ist optional. | |
| Aktualisieren der Einstellungen für den virtuellen Desktop | Aktualisieren Sie die Firewall-Policies und -Services für den virtuellen Desktop, um das vCenter Operations Manager for Horizon View-desktopspezifische Sammeln von Kennzahlen zu unterstützen. | |
| Erstellen der virtuellen Maschine für den vCenter Operations Manager for Horizon View Adapter-Server | Erstellen Sie eine virtuelle Maschine im vSphere-Client, die als vCenter Operations Manager for Horizon View Adapter-Server verwendet werden soll. | |
| Installieren des Gastbetriebssystems für den vCenter Operations Manager for Horizon View Adapter-Server | Installieren Sie Windows Server 2012 R2 als Gastbetriebssystem für den vCenter Operations Manager for Horizon View Adapter-Server. | |
| Installieren der VMware vCenter Operations Manager for Horizon View Adapter-Software | Führen Sie die Bereitstellung und Konfiguration der vCenter Operations Manager for Horizon View Adapter-Software durch. | |
| Importieren der vCenter Operations Manager for Horizon View-PAK-Datei | Importieren Sie die vCenter Operations Manager for Horizon View Adapter-PAK-Datei über die Hauptweboberfläche von vCenter Operations Manager. | |
| Überprüfen der VMware vCenter Operations Manager for Horizon View-Funktionen | Überprüfen Sie die Funktionen von vCenter Operations Manager for Horizon View mit dem virtuellen Desktopmaster-Image. | |

# Kapitel 5 Lösungsüberprüfung

In diesem Kapitel werden die folgenden Themen behandelt:

**Übersicht** ..... 62

**Checkliste nach der Installation** ..... 63

**Bereitstellen und Testen eines einzigen virtuellen Desktops** ..... 63

**Überprüfen der Redundanz der Lösungskomponenten** ..... 63

# Übersicht

Nachdem Sie die Lösung konfiguriert haben, führen Sie die Aufgaben in Tabelle 24 durch, um die Konfiguration und die Funktionen bestimmter Aspekte der Lösung zu überprüfen und dafür zu sorgen, dass die Konfiguration die zentralen Verfügbarkeitsanforderungen erfüllt.

**Tabelle 24. Aufgaben für das Testen der Installation**

| Aufgabe | Beschreibung | Referenz |
|---|---|---|
| Überprüfen der Installation mit der Checkliste nach der Installation | Überprüfen Sie, ob geeignete virtuelle Ports auf jedem virtuellen vSphere-Hostswitch vorhanden sind. | *Handbuch für vSphere-Netzwerk* |
| | Überprüfen Sie, ob jeder vSphere-Host auf die erforderlichen Datastores und virtuellen LANs zugreifen kann. | • *Handbuch für vSphere-Speicher*<br>• *Handbuch für vSphere-Netzwerk* |
| | Überprüfen Sie, ob die vMotion-Schnittstellen auf allen vSphere-Hosts korrekt installiert sind. | *Handbuch für vSphere-Netzwerk* |
| Bereitstellen und Testen eines einzigen virtuellen Desktops | Stellen Sie eine einzige virtuelle Maschine über die vSphere-Oberfläche bereit und nutzen Sie dabei die Anpassungsspezifikation. | • *Handbuch für vCenter Server- und Hostverwaltung*<br>• *vSphere-Handbuch für die Verwaltung virtueller Maschinen* |
| Überprüfen der Redundanz der Lösungskomponenten | Starten Sie nacheinander jeden Speicherprozessor neu und vergewissern Sie sich, dass die VMware-Datastores-Verbindung aufrechterhalten wird. | Überprüfen der Redundanz der Lösungskomponenten |
| | Deaktivieren Sie nacheinander jeden der redundanten Switche und überprüfen Sie, ob die Verbindung von vSphere-Host, virtueller Maschine und Speicherarray intakt bleibt. | Dokumentation des Anbieters |
| | Aktivieren Sie auf einem vSphere-Host, der mindestens eine virtuelle Maschine enthält, den Wartungsmodus und überprüfen Sie, ob die virtuelle Maschine erfolgreich zu einem alternativen Host migrieren kann. | *Handbuch für vCenter Server- und Hostverwaltung* |
| Provisioning der verbleibenden virtuellen Desktops | Stellen Sie Desktops über die verknüpften View Composer-Clones bereit. | *Administration von VMware Horizon View* |

## Checkliste nach der Installation

Die folgenden Konfigurationselemente sind wichtig für die Funktion der Lösung und sollten vor der Bereitstellung in die Produktion überprüft werden. Überprüfen Sie Folgendes auf jedem vSphere-Server, der als Teil dieser Lösung verwendet wird:

- Die vSwitche, die die Client-VLANs hosten, sind mit ausreichend Ports konfiguriert, um die maximale Anzahl virtueller Maschinen zu beherbergen, die ein Host beherbergen kann.
- Alle erforderlichen virtuellen Maschinenportgruppen sind konfiguriert und jeder Server kann auf die erforderlichen VMware-Datastores zugreifen.
- Eine Schnittstelle ist korrekt für vMotion konfiguriert. Weitere Informationen finden Sie im *VMware vSphere-Netzwerkleitfaden*.

Weitere Informationen finden Sie in den in Kapitel 6 aufgeführten Dokumenten.

## Bereitstellen und Testen eines einzigen virtuellen Desktops

Stellen Sie eine einzige virtuelle Maschine bereit, um den Betrieb der Lösung zu überprüfen. Überprüfen Sie, ob die virtuelle Maschine der entsprechenden Domain zugeordnet ist, Zugriff auf die erwarteten Netzwerke hat und es möglich ist, sich bei ihr anzumelden.

## Überprüfen der Redundanz der Lösungskomponenten

Zum Überprüfen, ob die verschiedenen Komponenten der Lösung die Verfügbarkeitsanforderungen erfüllen, ist es wichtig, bestimmte Szenarien zu testen, die für die Wartung oder Hardwareausfälle relevant sind.

1. Starten Sie alle VNX-Speicherprozessoren nacheinander neu und überprüfen Sie, ob die Verbindung zu VMware-Datastores während des Vorgangs aufrechterhalten wird. Führen Sie die folgenden Schritte aus:
   a. Melden Sie sich bei der Control Station mit Administratorrechten an.
   b. Wechseln Sie zu **/nas/sbin**.
   c. Starten Sie SPA neu. Verwenden Sie dazu den Befehl **./navicli -h spa rebootsp**.
   d. Überprüfen Sie während des Neustartzyklus die Präsenz von Datastores auf vSphere-Hosts.
   e. Starten Sie nach Abschluss des Zyklus SPB neu: **./navicli -h spb rebootsp**.
2. Führen Sie ein Failover jedes VNX Data Mover durch und überprüfen Sie, ob die Verbindung zu den VMware-Datastores aufrechterhalten bleibt und Verbindungen zu den CIFS-Dateisystemen wiederhergestellt werden. Verwenden Sie den folgenden Ansatz für jeden Data Mover und nutzen Sie die Unisphere-Benutzeroberfläche für den Neustart.
   a. Führen Sie an der $-Befehlsaufforderung der Control Station den Befehl **server_cpu *movername* -reboot** aus, wobei *movername* der Name des Data Mover ist.

b. Zum Überprüfen, ob die Netzwerkredundanzfunktionen erwartungsgemäß funktionieren, deaktivieren Sie nacheinander die redundanten Switchinginfrastrukturen. Während jede der Switchinginfrastrukturen deaktiviert ist, überprüfen Sie, ob alle Komponenten der Lösung die Verbindung miteinander und zu jeder vorhandenen Clientinfrastruktur aufrechterhalten.

3. Aktivieren Sie auf einem vSphere-Host, der mindestens eine virtuelle Maschine enthält, den Wartungsmodus und überprüfen Sie, ob die virtuelle Maschine zu einem alternativen Host migrieren kann.

# Kapitel 6 Referenzdokumentation

In diesem Kapitel werden die folgenden Themen behandelt:

**EMC Dokumentation** ..... **66**

**Andere Dokumentationen** ..... **66**

## EMC Dokumentation

Die folgenden Dokumente auf der EMC Online Support-Website bieten weitere und relevante Informationen. Der Zugriff auf diese Dokumente hängt von Ihren Anmeldedaten ab. Falls Sie auf ein Dokument nicht zugreifen können, wenden Sie sich an Ihren EMC Vertriebsmitarbeiter.

- *EMC VNX5200 Unified – Installationshandbuch*
- *EMC VNX5400 Unified – Installationshandbuch*
- *EMC VNX5600 Unified – Installationshandbuch*
- *EMC VSI für VMware vSphere: Storage Viewer – Produktleitfaden*
- *EMC VSI für VMware vSphere: Unified Storage Management – Produktleitfaden*
- *Konfigurationsarbeitsblatt für VNX Block*
- *VNX Installation Assistant for File/Unified – Arbeitsblatt*
- *VNX FAST Cache: ein detaillierter Überblick, White Paper*
- *TechBook: Verwenden von EMC VNX-Speicher mit VMware vSphere*
- *Bereitstellen von virtuellen Microsoft Windows 8-Desktops – Leitfaden zur Anwendung von Best Practices*
- *Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere*
- *EMC PowerPath Viewer – Installations- und Administrationshandbuch*
- *EMC VNX Unified: Best Practices für Performance – Leitfaden zur Anwendung von Best Practices*
- *EMC VNX VAAI NFS-Plug-in – Readme-Datei*

## Andere Dokumentationen

Die folgenden Dokumente auf der VMware-Website enthalten weitere und relevante Informationen:

- *Bereitstellungs- und Konfigurationshandbuch: vCenter Operations Manager 5.8*
- *VMware vSphere – Installations- und Einrichtungshandbuch*
- *VMware vSphere-Netzwerk*
- *Handbuch zur VMware vSphere-Ressourcenverwaltung*
- *VMware vSphere-Speicher – Handbuch*
- *vSphere-Administratorhandbuch für virtuelle Maschinen*
- *VMware vSphere-Handbuch für die Verwaltung virtueller Maschinen*
- *Handbuch für VMware vCenter Server- und Hostverwaltung*
- *Installieren und Verwalten von VMware vSphere Update Manager*
- *Vorbereiten der Update Manager-Datenbank*

- *Vorbereiten der vCenter Server-Datenbanken*
- *Management von Arbeitsspeicherressourcen in VMware vSphere 5.0*
- *Erste Schritte mit View*
- *Planung der View-Architektur*
- *Installation von View*
- *Szenarien für die Einrichtung von SSL-Zertifikaten für View*
- *Einrichten von Desktop- und Anwendungspools in View*
- *Verwalten der View Cloud Pod-Architektur*
- *Benutzerprofilmigration in View*
- *View Security*
- *Benutzerprofilmigration in View*
- *VMware Horizon 6.0 mit View* Versionshinweise
- *VMware Horizon View – Optimierungshandbuch für Windows 7 und 8*
- *Installieren und Konfigurieren von VMware Workspace Portal*
- *Migration von VMware Workspace Portal*
- *VMware Workspace Portal – Administratorhandbuch*
- *Einrichten von Ressourcen im VMware Workspace Portal*
- *VMware Workspace Portal – Benutzerhandbuch*
- *VMware vCenter Operations Manager – Administratorhandbuch*
- *VMware vCenter Operations Manager for View – Installationshandbuch*
- *VMware vCenter Operations Manager – Installationshandbuch*
- *Bereitstellungs- und Konfigurationshandbuch: vCenter Operations Manager*
- *VMware vShield – Administratorhandbuch*
- *VMware vShield – Kurzanleitung*

# Anhang A Konfigurationsarbeitsblatt

In diesem Anhang wird das folgende Thema behandelt:

**Arbeitsblatt für die Kundenkonfiguration ..... 70**

# Arbeitsblatt für die Kundenkonfiguration

Bevor Sie die Lösung konfigurieren, müssen Sie einige kundenspezifische Konfigurationsinformationen wie IP-Adressen, Hostnamen usw. erfassen. Tabelle 25 bis Tabelle 30 enthalten ein Arbeitsblatt, das Sie zur Aufzeichnung der Informationen verwenden können. Dieses Arbeitsblatt können Sie auch ausdrucken und dem Kunden als zukünftige Referenz überlassen.

Im Anhang zu diesem Dokument finden Sie eine eigenständige Kopie des Arbeitsblatts im Microsoft Office Word-Format. So zeigen Sie das Arbeitsblatt an und drucken es aus:

1. Öffnen Sie in Adobe Reader den Bereich **Attachments** wie folgt:
   - Wählen Sie **View › Show/Hide** › **Navigation Panes** › **Attachments**.
     *oder*
   - Klicken Sie auf das **Attachments**-Symbol (siehe Abbildung 17).

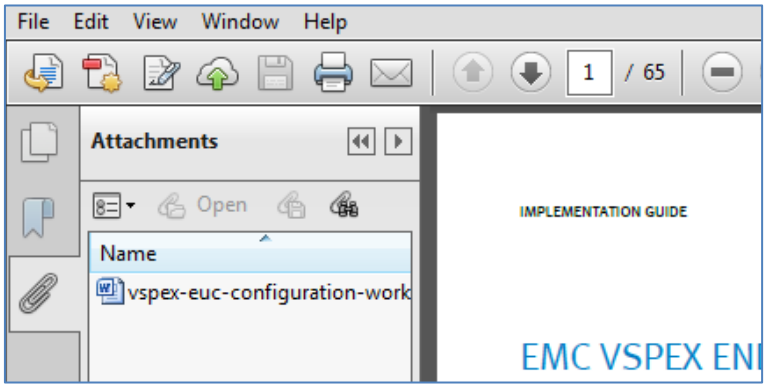


**Abbildung 17. Öffnen von Anhängen in einer PDF-Datei**

2. Doppelklicken Sie unter **Attachments** auf die angehängte Datei, um das Arbeitsblatt zu öffnen und auszudrucken.

Um die Kundenangaben zu bestätigen, überprüfen Sie das relevante Arraykonfigurationsarbeitsblatt: *Konfigurationsarbeitsblatt für VNX Block* oder *VNX Installation Assistant for File/Unified – Arbeitsblatt*.

**Tabelle 25. Allgemeine Serverinformationen**

| Servername | Zweck | Primäre IP |
|---|---|---|
| | Domaincontroller | |
| | Primäres DNS | |
| | Sekundäres DNS | |
| | DHCP | |
| | NTP | |
| | SMTP | |
| | SNMP | |
| | VMware vCenter-Konsole | |
| | VMware Horizon View Connection Server | |
| | VMware Horizon Workspace-Appliance(s) | |
| | Microsoft SQL Server | |
| | VMware vShield Manager | |
| | Managementserver für die Virenschutzlösung | |

**Tabelle 26. vSphere-Serverinformationen**

| Servername | Zweck | Primäre IP | Private Netzadressen (Speicher) | VMkernel-IP | vMotion-IP |
|---|---|---|---|---|---|
| | vSphere-Host 1 | | | | |
| | vSphere-Host 2 | | | | |
| | ... | | | | |

**Tabelle 27. Arrayinformationen**

| Feld | Wert |
|---|---|
| **Arrayname** | |
| **Administratorkonto** | |
| **Management-IP** | |
| **Name des Speicherpools** | |
| **Name des Datastore** | |
| **NFS-Server-IP** | |

**Tabelle 28. Informationen zur Netzwerkinfrastruktur**

| Name | Zweck | IP | Subnetzmaske | Standardgateway |
|---|---|---|---|---|
| | Ethernetswitch 1 | | | |
| | Ethernetswitch 2 | | | |
| | ... | | | |

**Tabelle 29. VLAN-Informationen**

| Name | Zweck des Netzwerks | VLAN-ID | Zugelassene Subnetze |
|---|---|---|---|
| | Clientzugriffsnetzwerk | | |
| | Speichernetzwerk | | |
| | Managementnetzwerk | | |

**Tabelle 30. Servicekonten**

| Konto | Zweck | Passwort (optional, angemessen gesichert) |
|---|---|---|
| | Windows Server-Administrator | |
| Root | vSphere-Root | |
| Root | Array-Root | |
| | Arrayadministrator | |
| | VMware vCenter-Administrator | |
| | VMware Horizon View-Administrator | |
| | VMware Horizon Workspace-Anbindungskonto | |
| Admin | VMware Horizon Workspace-Appliance – Administratorkonto | |
| Root | VMware Horizon Workspace-Appliance – Root-Konto | |
| Sshuser | VMware Horizon Workspace-Appliance – sshuser-Konto | |
| | SQL Server-Administrator | |
| | VMware vCOps-Administrator | |
| | VMware vShield Manager-Administrator | |